Cited Ref. 2

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－138664
（P2000－138664A）
(43)公開日　平成12年５月16日(2000.5.16)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
H04L	9/08		H04L	9/00	601C
G06F	12/14	320	G06F	12/14	320E
	17/60		G09C	1/00	620Z
G09C	1/00	620			640B
		640	G06F	15/21	Z

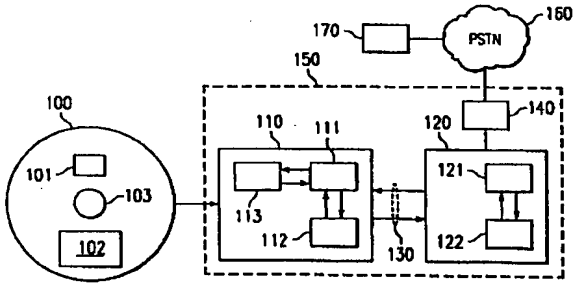
審査請求　未請求　請求項の数１　ＯＬ　（全 22 頁）

(21)出願番号　特願平11－214972
(22)出願日　平成11年７月29日(1999.7.29)
(31)優先権主張番号　１２９３７０
(32)優先日　平成10年８月５日(1998.8.5)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　398038580
ヒューレット・パッカード・カンパニー
HEWLETT－PACKARD COMPANY
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000
(72)発明者　ジェイ・ロバート・シンズ・サード
アメリカ合衆国80525コロラド州フォート・コリンズ、コネティカット・ドライブ　1936
(74)代理人　100081721
弁理士　岡田　次生

(54)【発明の名称】　公開キー暗号方式を利用したコンテンツの保護方法

(57)【要約】
【課題】　バルク格納装置に格納されるコンテンツを保護する方法を提供する。
【解決手段】　格納されたコンテンツの許可されていない利用を防止するための技術を公表することかできるので、保護コンテンツのマスターを作成したりコンテンツを新たに生成するのに適合したメディア装置の利用を可能にすることができる。本明細書では、特定のメディアの真正性検証や、受容されたメディア・プレイバック装置とメディア・コンテンツ・キーを安全に引き渡すためのこれらに対応する公開された公開キーのリストの利用や、メディア・コンテンツ・キー又は受容されたメディア・プレイバック装置の更新を提供する外部接続装置を含んだ、種々のコンテンツ保護方式を開示している。



1

【特許請求の範囲】
【請求項１】格納メディアに格納されたコンテンツの無権限の使用を防止するためのコンテンツ保護方法であって、
メディアの使用を許可された少なくとも１つの装置に関する情報を含んだ第１の情報を、該メディア上のアクセスが制限された部分に格納するステップと、
許可された前記少なくとも１つの装置の暗号キーを含んだ第２の情報を該メディア上に格納するステップと、
ユーザ・コンテンツを該メディア上のアクセスが自由な部分に格納するステップと、
特定のメディア使用装置が前記ユーザ・コンテンツを供給するのに受容可能なメディア使用装置であるか否かを、前記第１の情報の少なくとも部分的に参照することによって判断するステップと、
前記特定のメディア使用装置が前記判断ステップにおいて受容可能と判断されたか否かを含んだ情報を、前記第２の情報に含まれる前記暗号キーで暗号化して、前記特定のメディア使用装置に転送することによって、前記特定のメディア装置が前記ユーザ・コンテンツの少なくとも一部を使用することを可能にするステップと、を含むコンテンツ保護方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、記録メディア（媒体）に格納されたコンテンツについてのコンテンツ保護方法及び保護システムに係り、特に、記録メディア自身に格納された公開キーを用いて記録メディア上のコンテンツの使用を制御するコンテンツ保護方法及び保護システムに関する。
【０００２】
【従来の技術】現在、バルク（大規模）メディア上に記録されたコンテンツに対するアクセスを制御する若しくは安全にすることに置き換わる、様々な手法が提供されている。しかしながら、これら従来の手法の場合、セキュリティを維持するために手法自体を秘密状態に保つ必要があるという欠点を伴うことが多い。したがって、これら従来の手法では、秘密を厳守するためには、信用しうる当事者内のみで実装しなければならない。同様に、これらの手法は、該手法に用いる暗号キーに関する総合的な秘密性に依存することがしばしばある。このような暗号キーを公開することは、同様の手法を用いる全ての団体あるいは大部分の団体がセキュリティを失うことにつながりかねない。
【０００３】例えば、ＤＶＤメディアは、現在はビデオ・コンテンツに対する保護しか行っていないが、２部構成の手法を用いている。メディア上に記録された情報を復号化するための暗号キーは、予め定義されているプロトコルに従って生成され、且つ、メディア上のアクセスが制限された部分に同プロトコルに従って格納される。

2

また、このプロトコルでも定義されている暗号化技術は、プレイバック・事業体にキーを安全に渡す際にも利用される。したがって、例えばメディア・プレーヤのようなメディア装置若しくはメディア自体を製造するためには、この手法全体すなわちどのように動作するかを完全に理解する必要がある。さらに、同じ手法で予め定義されているキーに、製造業者が自らアクセスしなければならない。プレーヤを製造する全ての人々、及び、メディアを製造する全ての人々の間で広汎に秘密を守らなければならない。セキュリティを維持することは、暗号キーをどのように生成し、このキーを渡すためのメッセージをどのように暗号化するかということを秘密に保つことに依存している。もし、プロトコルそれ自身が暴かれたら、そのプロトコルによって生成され記録されたエンティティが何であれ、全てのコンテンツは危険にさらされる。何故ならば、プロトコルが一般常識になってしまうと、不心得者は保護されたコンテンツを復号化可能なキーを生成し、及び／又は、キーを横取りすることができるであろう。システムに対するいかなる妥協も、同時に全てのシステム及びメディアに対する妥協を招来することにつながる。
【０００４】付言するならば、保護コンテンツに関連するメディア・コンテンツ・キーがメディア自体に格納されているので、上述のシナリオはキーのセキュリティを知り得るシステムの全パートに全て依存する。それゆえ、メディア読取装置を不法にデザインすることによって、キーを受け取る権限がない装置又は事業体にコンテンツ・キーを渡すことができる。同様に、メディア読取装置を不法にデザインすることによって、メディアに格納されている暗号化されたコンテンツとメディア・コンテンツ・キーを含んだまま、メディアの生データを２次的なメディア上にコピーすることによって、上述のプロトコルに準拠した不正コピーを作成することができる。
【０００５】しかしながら、全ての生データを利用できる訳ではないので、この手法に従ったメディア読取装置は、このような不正アクセス／動作を防止してセキュリティを提供することができるであろう。特に、一般消費者向けの全ての製品では、キーが隠されているセクタは利用することができないようになっている。何故ならば、この種の全ての製品は、この手法を用いる場合には装置は特定の動作を許容しないようにすることを条件としたライセンスの下で製造されるからである。
【０００６】したがって、コンテンツの保護を提供するシステムでは、メディア上に格納されたメディア復号化キーは、メディア読取装置によって、適切な環境下でのみ読み取られる。例えばＤＶＤディスク・ドライブのようなメディア読取装置の場合には、正当なプレイバック装置が予め確立されたプロトコルに従ってメディア・コンテンツ・キーを要求し、これに対して、通信のために暗号化された形式でプレイバック装置に供給される。こ

の手法では、メディア･コンテンツ・キーは、キー交換の後で渡されるようになっている。したがって、メディア読取装置からプレイバック装置にキーが渡されるときに、キーは暗号化される。すなわち、プレイバック装置は、メディア読取装置に対して暗号キーを送信し、メディア読取装置はメディアからメディア･コンテンツ・キーを読み取り、プレイバック装置の暗号化キーを用いて該メディア・コンテンツ・キーを暗号化して、メディア･コンテンツ・キーの当該暗号化バージョンをプレイバック装置に渡する。したがって、メディア読取装置から供給されるメディア･コンテンツにアクセスする際にメディア･コンテンツ・キーを使用するためには、プレイバック装置の復号化キー（秘密裏に保持されている）によって復号化することができる。

【０００７】例えば、コンピュータのバス構造を介してＤＶＤディスク･ドライブ（メディア装置）を接続したホスト･コンピュータ（ここではプレイバック装置とする）では、コンピュータとドライブ間で交換される情報は、不心得者、若しくは「ハッカー」がバス上の動作をプローブで検出することによって、いとも簡単にあばかれる。したがって、メディア･コンテンツ・キーは、ドライブとホスト･コンピュータ間でのキー交換を介して確定されたキーによって隠されているときのみ、このバスを経由して渡される。これに対し、スタンドアロンのプレーヤの場合、メディア読み取り機構とビデオ再生装置が同一の筐体内に収納されているので、両者間の接続は幾分安全であり、それゆえ、データを内部的に直接復号化する場合には、キー交換及び／又はメディア･コンテンツ・キーの暗号化を省略することができる。

【０００８】この手法を実装する方法は、メディア読み取り装置自身がメディア･コンテンツ・キーにアクセスするので、この手法を実現するとともに、不正目的のためのコンテンツ・キーへのアクセスを拒絶しなければならない。同様に、プレイバック装置にはコンテンツ・キーが供給されるので、プレイバック装置も当該保護方法を実現できなければならない。しかしながら、キーの不正や取り出しや横取りを避け、セキュリティを維持するためには、個々のキーのセキュリティに依存するのに加えて、何処にどのようなフォーマットのコンテンツ・キーが書き込まれているかや、キー交換動作のためのアルゴリズム等といった、上記した手法自体の処理動作の詳細自体も、セキュリティを保たなければならない。さらに、現在に手法のままでは、もし事業体が適法な保護メディアを生成することができるならば、適法な保護メディアの生成を許容するために、該手法に関する秘密はこの事業体に必然的にあばかれてしまうので、該事業体は、他のメディアの不法コピーも生成することができる。

【０００９】したがって、データ暗号化とキーの生成のプロトコルは、ライセンスのみによって見ることができる。すなわち、信用されたコンテンツ製造業者と、コンテンツを読み、書き、あるいは他の利用を行う装置の製造業者にのみ、プロトコルに関する秘密が供給されるが、この秘密情報の使用や拡散を禁止するライセンス同意書の文言によってしか秘密が保証されない。ごく少数の人又は事業体が、当該プロトコルに準じたコンテンツ及び／又は装置アダプタを供給するために、このようなライセンスやこれに付随する秘密を取得することができる。一般的なコンテンツ提供業者は、小さな事業体であったり、内部的又は限定的な使用のためにコンテンツを供給する事業体であったりする。このような事業体は、保護コンテンツの不法なコピーや使用を防止することができるキーをメディアに安全な方法で記録する方法を持たない。したがって、これら事業体に対してセキュア（安全）なディスクの合法な生成を許可（オーソライズ、権限を与える）しても、彼らは製品を保護することはできない。したがって、このようなキーを生成するために公に使用することができるような処理方法は存在しない。すなわち、上記した手法と互換な保護コンテンツを記録するライセンスを受けた事業体以外の者が利用可能な処理方法は存在しないのである。

【００１０】

【発明が解決しようとする課題】本発明の目的は、メディア上に格納されたキーを安全に引き渡し、外部のオーソリゼイション･センタと通信し、メディアの真正性を検証することができる、コンテンツのアクセスに関する代替技術を提供することにある。

【００１１】本発明の更なる目的は、セキュリティを妥協する危険なしに、大勢の人やエンティティ（事業体）によって利用可能な、マス･メディアのコンテンツに対する安全なアクセスを提供する技術を提供することにある。

【００１２】

【課題を解決するための手段】上述あるいはそれ以外の本発明の目的、構成、技術的な利点は、本発明に係るシステムや方法を利用することによって達成される。本発明に係るシステムや方法それ自体は公開することができる。但し、ここで用いられる個人のキーだけはプライバシーを保つ必要がある。システムの保護を欲する全ての人に対して利用可能にするためには、本発明に従った実施に適合したキーを生成するルールは、公にすることが好ましい。本発明に係る技術それ自体は、本発明で用いられる暗号キーを生成するためのルールと同様に公表されるので、本発明は、望む全ての人に対して使用を許可することができる。さらに、本発明によれば、セキュリティを保つためには、暗号キー自体若しくはその一部は安全に維持されるが、穂は発明において実施される技術に関する秘密性には依存しない。すなわち、本発明において秘密情報を危険にさらすことは、コンテンツにアクセスするための特定のキーを使用するコンテンツ提供業

者のみに対して秘密情報が危険にさらされることにしかならない。

【００１３】本発明は、暗号キーの使用を通して、コンテンツへのアクセスを制限することに加えて、これを保護するように動作する。特に、本発明によれば、メディアの一片がオリジナルと同一であるかどうかを安全に同定することができる。同様に、本発明によれば、プレイバック装置が許可されているかどうかを安全に同定することができる。したがって、メディア装置又はメディアのユーザは、各一端は他端を安全に同定し、且つ、各一端は他端に対して安全にデータを送信することができるものとして、対話が許可されていると仮定することができる。

【００１４】本発明に係る動作は、いかなる特定の伝送をも許可又は禁止するものではなく、むしろ、暗号化方法を用いてコンテンツ（情報又はデータ）を不明瞭にするものである。したがって、合法的な受信者のみがデータを利用することができる。すなわち、コンテンツの所有者や該所有者によって許可された以外の者は誰も、保護されたメディア･コンテンツをコピーすることができない。本発明によれば、一端では、本発明において有効な暗号キーを提供するために、当該技術分野において広く知られている公開キー・アルゴリズムを利用する。しかしながら、本発明は、このような暗号キーを管理し利用するための固有のシステムや方法をも提供するものである。

【００１５】上述した先行技術に関するシステムと同様に、メディア読み取り装置又はディスク･ドライブ（メディア装置）は、本発明に係る技術を熟知することが好ましい。例えば、メディア装置の製造業者のライセンスを通して、これら装置は本発明に係る技術を熟知することができる。したがって、前述したコンテンツ・キーのような高度に極秘の情報を、該情報が公に拡散されてしまうといった実質的な懸念なしに、メディア上に格納することができる。当該手法を認知しないメディア装置はメディアを攻撃することはない。すなわち、未加工の標準領域を読み書きできるドライブは、安全領域に書き込まれたコピー保護情報をコピーしようとしたりしない。したがって、メディア上に格納された極秘の情報を読むなどのような、本発明に係る技術を破ろうとするいかなる企ても、当該技術を達成することはできない。すなわち、メディア読み取り装置に対してメディアの禁止領域へのアクセスを命令することはできない。また、もしメディア読み取り装置が不適切な使用を許容したとしても、法的な救済が可能である。

【００１６】しかしながら、手法そのものを秘密にする従来技術に係るシステムとは相違し、本発明では、技術に関するライセンスを取得する必要がなく、また、自ら生成することはない秘密情報をも必要とせずに、自分自身の保護コンテンツを公に大々的に生成することができる。何故ならば、本発明に係る技術によれば、キーそのもののみが秘密であり、キーを生成するためのルールを公にすることができるからである。したがって、メディア読み取り装置は、本発明に従って保護されたコンテンツのマスターを生成するために、メディア中の安全領域に対する限定的なアクセスを許容することができる。このことにより、誰もが自分自身の保護メディアを生成することができる。

【００１７】本発明によれば、公開キーとの秘密キーの組が使用される。秘密キーは、デコーダ若しくはプレイバック装置の選択又は許可を行うために、製造業者若しくはコンテンツ提供業者のみが知っている。したがって、個々の装置、関連する一連の装置、又は、製造業者の装置は、装置自身のみが知る異なる秘密キーを利用することができる。同様に、本発明の好ましい実施形態では、各メディアは互いに異なるコンテンツ・キーを知っている。もし危険にさらされることがあるならば、該当するメディアのセキュリティに対する危険のみである。

【００１８】しかしながら、メディア、又は、メディアが厳密に受動的な装置として稼動するメディア装置は、プレイバック装置が持つ公開キーを知る必要がある。公開キーが実際に特定の所有者に帰属するということがメディアに対して保証されている、すなわち、メディアが真正なもので認可され許可された装置と関連付けられている限りにおいては、システムは安全であると言える。したがって、プレイバック装置の所有者若しくは製造業者は、事実、公開キーを内輪で秘密状態に保つことによってではなく、これを世界中に拡散することによって、最も好適に作用する。このように公開キーを公に拡散することによって、不心得者があたかも認可され許可された事業体に帰属するものであるかの如くに偽って公開キーを配布するような機会を減じることができる。例えば、会社Ｘが、それ自身が公開キーのソースであることを表示して公開キーを広く公表すれば、その後に会社Ｚが、以下の公開キーが会社Ｘの公開キーであるかように公衆をだまして信じ込ませることは極めて難しくなる。したがって、本発明の実施形態では、認可されたプレイバック装置の公開キーは、実際にメディア上で公開することが好ましい。

【００１９】プレイバック装置の公開キーを公表することによって、本発明は、情報の伝送を安全に行うことができるだけでなく、一端又は両端、すなわちメディアとプレイバック装置の一方又は双方が合法的であることを、安全に識別することができる。したがって、完全に可読な領域とアクセスが制限可能又は禁止された領域とを提供するいかなる情報格納方法も、本発明によって利用可能となる。

【００２０】前述した従来技術に係る手法とは相違し、広い範囲、すなわち、当該手法の動作を完全に知る必要があるプレイバック装置の提供業者とメディア生成提供

業者の間で、キーの値を含めて、秘密を保つ必要は全くない。本発明では、秘密キー自身を秘密にするだけで充分なので、大掛かりな団体の間で秘密を共有する必要は全くない。したがって、各製造業者は、メディアの製造業者であれ、メディアを装填して動作する装置の製造業者であれ、自分自身の秘密を保持するだけで充分である。さらに、各製造業者の秘密は保持されるので、真の秘密はごく少数の人々の間でのみ知り得るものとなる。この結果、真実の秘密を誰も実際に知ることができない。例えば、秘密は乱数生成によって組み込まれ出荷されて、書き取る前に破壊されたり、あるいは、キーに関する断片的な情報が所定の人々に与えられ、このうちの一部の人達がキーを再構築することを余儀なくされた結果として秘密が葬り去られたために、真実の秘密を現実に誰も知ることができないといった具合である。さらに、本発明によれば、各々の秘密キーは、暗号化／復号化情報として回路の中に組み込むこともできるので、秘密キーがいかなる人にも暴かれることはない。

【００２１】本発明の代替的な実施形態では、コンテンツ・キーをメディア中のアクセス制限領域に格納するのではなく、メディア装置によって読み取られ、次いでプレイバック装置へ転送される間、メディア装置に対してキーを決して開示することなくプレイバック装置にキーを安全に伝送するように実際に動作するメディアによってキーが安全に格納される。したがって、このキーを隠蔽するために使用される実際のコンポーネントは、メディア装置又はディスク･ドライブのいずれにも存在しない。その代わりに、内部アルゴリズムの制御下で動作するプロセッサとメモリを含んだ電子回路のような、メディアの一部が、キーの隠し場所となる。この場合、コンテンツ・キーは、前述したメモリ内のメディア上に格納されているので、メディア装置からプレイバック装置に渡されるプレイバック装置の公開キーを好適に用いることによって、メディア装置にあばかれることなく、隠蔽することができる。上述した、プレイバック装置の安全な同定方法によれば、この代替的な実施形態における現実のメディアは、メディア・キーが許可されていない事業体によってあばかれることがないと仮定することができる。あるいは、コンテンツ・キーは許可されたプレイバック装置に関する公開キーを用いて暗号化されているという事実により、秘密キーのセキュリティ侵害がなければプレイバック装置によってのみ使用可能であることが保証される。

【００２２】本発明の他の代替的な実施形態によれば、「ペイ･パー･ビュー（pay per view：見る度に課金する）」と呼ばれるような、コンテンツ・キーを取得するための外部ソースを利用することができる。したがって、メディア上に格納したコンテンツ・キーを用いるのではなく、メディアの真正性を確認するために使用することができる識別ストリングを格納しておき、本発明に従った公開キー暗号化を利用して外部ソースにこの識別ストリングを供給することができる。この結果、要求するコンテンツとともに有効なコンテンツ・キーを得ることができる。

【００２３】付言しあるいは換言するならば、外部ソースにアクセスすることによって、メディアの使用に適していると許可されたデコーダ若しくはプレイバック装置に関する最新の情報を得ることができる。例えば、許可された公開キーのリストは、このような通信によって更新される。この結果、メディア装置は、最初は許可されていなかったデコーダに対してコンタクト・キーを安全に供給することができる。

【００２４】本発明の技術的な利点は、本発明を実現するための技術自体は広く知られているという点である。したがって、広汎に利用することができ、保護コンテンツのコピーを有効に防止することができる。

【００２５】また、本発明の更なる技術的利点は、後で許可された装置においてプレイバックが許容になるのと同様に、専用プレーヤとコンピュータの双方において再生動作が許容されているという点である。

【００２６】また、本発明の更なる技術的利点は、ビデオ情報とコンピュータ情報の双方の保護に対して適用可能である点である。さらに、かかる保護が実現することによって、電話回線やインターネットのように一般に利用可能な通信ネットワーク経由で、外部オーソリゼイション（許可）センタとの対話、例えば「ペイ･パー･ビュー（観る毎に課金する）」、が可能となる。

【００２７】これまでの記述は、本発明の特徴や技術的な利点に関して、概略的且つに広義に説明したものである。以下に続く本発明に関する更に詳細な記述を参照することによってより深く理解することができる。以下では、本発明のクレームの要旨を形成するような本発明に関する付加的な特徴や利点が記述されている。当業界で通常の知識を有する者であれば、開示された本発明の概念や特定の実施例を基にして、本発明と同一の目的を実現するための他の構造に修正したりデザインしたりすることができるが充分理解できるであろう。また、当業界において通常の知識を有する者であれば、このような均等な構造は、添付の特許請求の範囲にクレームされた本発明の要旨や権利範囲を逸脱しないということも充分理解できるであろう。

【００２８】

【発明の実施の形態】本発明の要旨を理解する上で、本発明が利用されている特定の実施形態を参照することが役に立つ。したがって、以下では、デジタル･システムによる使用に適した情報、例えばＤＶＤ光ディスク上に格納されるようなデジタル･ビデオ情報、を格納するためのバルク･メディアにおいて本発明が利用される実施形態について説明することにする。しかしながら、本発明は、かかる実施形態に限定されるものではなく、事

実、コンテンツに対する安全な又は制限されたアクセスを行うような記憶領域を提供するためのいかなる情報蓄積手法に対しても本発明を適用し得るということを充分理解されたい。

【００２９】図１には、本発明を適用したシステムを示している。該システムは、メディア１００と、メディア装置１１０と、プレイバック装置１２０とで構成される。メディア１００は、格納情報に対する一般的なアクセスを許容する非保護記憶領域１０２と、格納情報に対して安全で制限されたアクセスしか許容しない保護記憶領域１０１とを含んでいる。本発明の好ましい実施例では、保護記憶領域１０１は、本発明に係る技術を実現したメディア装置が本発明に従ってアクセスする以外には情報へのアクセスを許容しないような、メディア１００中の所定の領域である。本発明の他の実施例では、保護記憶領域１０１は、活動的な領域であり、すなわち、本発明に従ってアクセスする以外には情報へのアクセスが許容しないようなプロセッサ･ユニットとこれに関連する制御アルゴリズムなどによって格納されたデータに対する自立的な制御を格納している。

【００３０】また、図１から判るように、メディア装置１１０は、例えば、光学的あるいは磁気的なディスク装置であり、メディア１００を装填して、情報を読み及び／又は書きするなどのような相互作用を実現することができるようなっている。メディア装置１１０は、例えば磁気ヘッド、若しくはレーザとフォト･ダイオードの組み合わせなどからなるインターフェース１１３を備えており、メディア装置１１０とメディア１００間での相互作用によりメディア１００とのインターフェースを行えるようになっている。インターフェース１１３は、プロセッサ１１１と接続している。プロセッサ１１１は、インターフェース１１３経由でメディア１００から供給される情報を受け取ったり、インターフェース１１３経由でメディア１００に情報を供給するだけでなく、インターフェース１１３の動作に対する制御を実行することができる。例えば、メディア１００が当業界において周知のディスクである場合には、コントローラ１１１がインターフェース１１３の変位を制御することによって、インターフェース１１３はメディア１００上の所望の物理ブロック及びセクタに対してアクセスすることができる。

【００３１】プロセッサ１１１にはメモリ１１２も接続されている。メモリ１１２は、メディア装置１１０に関する数々の機能を提供することができる。例えば、メモリ１１２には、上述したようなインターフェース１１３の変位制御を本発明に従って動作せしめるために、ＣＰＵ１１１により利用される制御プログラムを格納することができる。さらに、メモリ１１２は、暗号キーや安全な転送のための暗号化を処理したりするといったメディア装置１１０の有効な機能のための環境を提供するだけでなく、プレイバック装置１２０とメディア１００の間で交換される情報を一時格納（バッファ）するために利用することができる。

【００３２】図１に示すプレイバック装置１２０は、バス１３０経由でメディア装置１１０と接続することで、プレーヤ１５０を構成している。プレイバック装置１２０には、プロセッサ１２１が含まれる。このプロセッサ１２１は、メディア装置１１０経由でメディア１００から供給される情報を受信したり、メディア装置１１０経由でメディア１００に情報を供給するだけでなく、メディア１００に関する情報を配布したりあるいは受け取るように動作することができる。例えば、プロセッサ１２１は、メディア１００上に記録された情報をプレイバック装置１２０に接続されたモニタ（図示しない）上で再生するように動作することができる。同様に、プロセッサ１２１は、メディア１００上に記録すべき情報を、プレイバック装置１２０に接続されたユーザ･インターフェース（図示しない）から受け取るように動作することができる。

【００３３】プロセッサ１２１には、メモリ１２２も接続されている。メモリ１２２は、プレイバック装置１２０の処理動作に関する数多くの機能を提供することができる。例えば、メモリ１２２には、プロセッサ１２１が本発明に従って動作するための制御プログラムが格納されている。さらに、メモリ１２２は、プレイバック装置１２０に供給されたメディア･コンテンツに関する暗号キーや復号化を処理するといったようなプレイバック装置１２０の有効な機能のための環境を提供すると同様に、プレイバック装置１２０とメディア１００の間で交換される情報を一時格納することができる。したがって、プロセッサ１２１とメモリ１２２は、メディア１００のコンテンツを好適に利用するためのデコーダとして動作することができる。

【００３４】メディア装置１１０とプレイバック装置１２０を連結するバス１３０は、例えば、パーソナル･コンピュータ（ＰＣ）における入出力（Ｉ／Ｏ）バスのような、安全でないバスであってもよい。この場合、メディア装置１１０はディスク･ドライブに相当し、プレイバック装置１２０はＰＣに相当する。しかしながら、バス１３０に対してセキュリティをかけることによって、メディア装置１１０とプレイバック装置１２０はともに、実質的に安全な環境に置かれる。例えば、プレーヤ１５０を、テレビジョン上に設置されるＤＶＤプレーヤのように、ユニット内に収容するといった具合でよい。このような環境下では、メディア装置１１０のプロセッサ１１１とプレイバック装置１２０のプロセッサ１２１を単一のプロセッサとして構成することができる。同様に、メディア装置１１０のメモリ１１２とプレイバック装置１２０のメモリ１２２を、単一のメモリとして構成することができる。

【００３５】図１では、一般公衆回線（ＰＳＴＮ）１６０経由でクリアリング･ハウス１７０と接続するオプション的な通信装置１４０が、プレイバック装置１２０に接続されている。通信装置１４０は、例えば「ペイ･パー･ビュー」方式のサービスにおける、プレイバック装置１２０とメディア１００との間の特定のトランザクションを許可するだけでなく、プレイバック装置１２０やメディア装置１１０に格納されている情報を更新するために利用することができる。更新される情報は、例えば、許可されたデコーダ及び／又はこれらに関係する公開キーに関するリストである。プレイバック装置１２０に直接接続されているように図示しているが、通信装置は、例えばメディア装置１１０に接続されるなど、当該システム内で別の箇所に接続されていてもよい。同様に、クリアリング･ハウス１７０とはＰＳＴＮ１６０経由で連絡しているように図示しているが、例えばローカル･エリア･ネットワーク（ＬＡＮ）、ワイド･エリア･ネットワーク（ＷＡＮ）、インターネット、ケーブル･システム、衛星放送システムのようなその他数多くの通信リンク経由で通信が果たされていてもよい。

【００３６】上述したように、メディア１００の好適に保護された記憶領域は、其処に格納されている情報へのアクセスが安全又は制限された領域である。例えば、本発明の好ましい実施形態では、保護格納領域１０１は、例えばメディアの有効領域中の先頭セクタ又は最終セクタといったような、メディア上の予め定義された領域であり、メディア装置１１０は一般的なアクセスを許容しない。この保護格納領域１０１へのアクセス禁止は、本発明に係る技術を知り得るメディア装置１１０の製造業者の同意によって達成される。

【００３７】あるいは、保護格納領域１０１へのアクセス制限は、典型的な従来世代のメディア装置では物理的にも一般的にもアクセスすることができない標準的なメディアの部分へのアクセスを可能にするようにメディア装置１１０を改良するとともに、本発明に係る技術を知り得る製造業者の同意を得てメディア装置１１０によるメディア･アクセスを制限することによっても達成される。後者の代替技術によれば、特に本発明に従って動作するように設計されていないメディア装置による物理的アクセスが防止されているという点において、保護格納領域１０１の情報に関するさらなるセキュリティが提供される。しかしながら、この代替技術の欠点は、本発明に従って保護されたメディアは、本発明に準拠していないメディア装置上での利用には適していないという点である。

【００３８】本発明の代替的な実施形態では、保護格納領域１０１は、プロセッサやこれに関連するメモリによって提供されるような、メディア１００の活性部分である。したがって、本発明に従って利用される暗号キーのような情報は、選択された条件の下でしか、格納したり外部に供給したりすることができない。したがって、本発明に係る技術を知り得るメディア装置に対する信頼は避けられ、その代わりに、メディア自身の安全な活性領域と置き換えられる。このようにして、メディア装置の情報が暴かれたり、このような秘密を利用する能力をメディア装置に与えることなく、暗号キーやその他の極秘情報の供給をメディア装置経由で許可されたプレイバック装置に転送することができる。それゆえ、メディア自身の活性部分は当該機能を実現することができるが、この点は、これらの機能を実現するメディア装置との関連で後述する。

【００３９】メディア１００のこのような活性部分は、メディア装置１１０内に配設された補助接続部と接続するように配設された、メディアの中央ハブ部分（図１中のハブ１０３）に設けられた電気接続部を経由して、メディア装置１１０及び／又はプレイバック装置１２０とデータ交換するためのインターフェースを実現することができる。勿論、このような実施形態では、メディア１００を適合させるだけでなく、メディア装置１１０も本発明に従った処理動作を備える必要がある。これに代わって、メディア装置の未変更のメディア･インターフェースによってメディア装置１１０と相互作用を実現するように配置されている活性コンポーネントを持つ表面領域を含むようにメディア１００を変更することができる。例えば、メディア１００が磁気メディアである場合、保護領域１０１には、メディア１００のセクタ又はトラックに沿って配設される磁気読み／書きヘッドのコイルと同様に、メディア装置１１０が可読な磁気パターンを生成するとともに、メディア装置１１０によって書き込まれた磁気パターンを受信して選択された情報を通信するように本発明に従って制御可能な回路を含めることができる。また、メディア１００が光ディスクである場合には、保護領域１０１には、メディア１００のセクタ又はトラックに沿って配設される光照射ダイオード及びフォト･ダイオードと同様に、メディア装置１１０に可読な光パターンを生成するとともに、メディア装置１１０によって書き込まれた光パターンを受信する回路を含めることができる。

【００４０】メディア１００の活性部分は、公開キー・アルゴリズムを含んだ集積回路、若しくは“チップ”のようなコンポーネントの形態で提供される。したがって、このような回路の中に、秘密キーを予め埋め込んでおくことができる。このようにすれば、チップを暴かない限り、秘密キーをチップ外部から利用することができなくすることができる。公開キーと秘密キーを用いた暗号化の基本は、もし秘密キーを知っていれば、対応する公開キーによって情報を復号化することができるというだけである。それゆえ、秘密キーを知る必要は全くない。秘密キーが真正であるか否かは、乱数を生成し、これを公開キーで暗号化して暗号情報としてチップに送信

し、チップがこの秘密キーを用いて元の乱数に復号化させてみて、秘密キーを用いて乱数を再び暗号化してみることによって検証することができる。もし、戻されてきた暗号列を公開キーで復号化することによって乱数が現れたならば、チップ内で使用されている秘密キーは有効であると断言できる。

【００４１】上記したような乱数の交換は、通信のいずれの端末側においても有効化に利用することができる、ということを理解されたい。さらに、発行者のキーに対応するキーを受信者が持っていることを証明するためには、ただ1回の暗号化及び復号化サイクルを経るだけで充分である。しかしながら、復号化された乱数を再度暗号化するためには、受信者が正しい乱数を単純に推測しないという高いレベルの確信が必要である。

【００４２】上記では乱数の使用について言及してきたが、上述したような検証や、以下で説明するような情報を偽造する技術には乱数以外の情報も利用することができるということを理解されたい。例えば、時刻及び／又は日付情報などの情報の特定のパターンを利用することができる。同様に、ハッシュ、又は、データを固有な形式で変更することかできる他のアルゴリズムを通じて得られる特定の情報ランを用いることもできる。勿論、より「ランダム」又は予測不能なデータを用いることで、受信者による推測可能性はさらに低下する。

【００４３】本発明の他の代替的な実施形態では、保護領域１０１は、メディア１００の区別可能な領域ではなく、メディア１００の非保護領域内で安全な形式で提供される。例えば、保護すべき若しくはアクセスを制限すべき情報を、修復が不可能であるか又は本発明に従って動作する装置を除いては修復できないように、非保護領＊域１０２全体を撹乱してもよい。また、本発明のある実施形態によれば、保護領域１０１に格納された情報は、非保護領域１０２に格納された情報中のエラーとして符号化される。このようなエラーは、例えば当業界において周知のＣＲＣエラー訂正アルゴリズムによって訂正可能なことが予め判っているので、非保護領域１０２中に格納された情報をエラー無しで供給することができる。しかしながら、このようなエラー及び／又はエラーの特定パターンの配置は、保護領域１０１の情報の符号化に利用される。生データ以外を提供するシステムはコピーする前にエラーを「訂正」するＣＲＣアルゴリズムを使用するので、このような実施形態は不正なコピーを防止するのに利用することができる。

【００４４】上述の代替的な実施形態に拘らず、保護領域１０１を提供する実施形態と組み合わせることができる点を理解されたい。例えば、保護領域１０１の情報の一部分は、上記したうちで異なる実施形態に従って格納してもよい。同様に、保護領域１０１の全ての情報が、上記実施形態の各々によって格納されてもので構成されてもよい。この場合、メディア装置及び／又はプレイバック装置との最大限の互換性が提供される。

【００４５】保護される情報の格納に関する実施形態について述べてきたので、保護領域１０１に格納される情報に関する好ましい実施形態を理解するためのテーブルを以下に示しておく。テーブル中の全ての値は、好ましくはリトル･エンディアン・フォーマットで記録されている。

【００４６】

【表１】

オフセット	サイズ	名前
0	１２８	１０２４ビットのメディア･キー（ｎ）
１２８	１２８	予約
２５６	１２８	１０２４ビットのメディア･キー（ｅ）
３８４	１２８	予約
５１２	4	デコーダ･キー･ファイルＣＲＣ
５１６	１２	予約
５２８	8	ディスク･キー
５３６	8	予約
５４４	1	ＳＣＭＳカウント
５４５	1	暗号タイプ
５４６	1	公開キー・フラグ
５４７	1	地域コード
５４８	2	キー拡張数
５５０	２６	予約
５７６	Ｎ＿Ｋ＊８	キー拡張

【００４７】メディア･キー（ｎ）は、好ましくは１０２４ビット･キーであり、メディア･キー（ｅ）も好ましくは１０２４ビット･キーであるが、各々はメディア公開キーの片方に相当する。以下では、このキーの生成と利用について説明する。

【００４８】メディアは、デコーダのリストを有していることが好ましい。本発明の好ましい実施形態では、メディアは公開キー・フラグによって識別され、著作者は

メディアの使用を受容し得るとみなされる。したがって、公開キー・フラグは、許可されたデコーダと関連付けて、ディスク･キーを送信することが許可されたドライブの公開キーがどれであるかを示す。もしこのビットが以下のテーブルに示すようなセットであれば、ドライブは、レポート･キー･コマンドに応答して、対応する公開キーによって暗号化されたディスク･キーを返すことを許可する。

【００４９】

【表２】

ビット	説明
0	ディスク･キーの報告のためにキー･セクター中の公開キーを有効にする
２－６	予約
7	何処にもリストされていない公開キーは受理可能である

【００５０】本発明の好ましい実施形態では、公開キー・フラグによって許可できると指示された公開キーは、メディア自身に格納して、キー拡張によって示されている。各キー拡張エントリは、３２ビットの符号無し整数の組であることが好ましい。最初の整数は、許可されたデコーダ･キーのセクター番号を示し、２番目の整数は、該デコーダ･キーのバイト･カウントを示す。キー拡張数には、キー･ファイルを含む拡張数が書き込まれる。読み出し専用メディアの場合、この数は１であることが好ましい。

【００５１】本発明によれば、コンテンツの著者又は提供業者は、会社Ｘ、Ｙ、及びＺの製品をレビューして、それら製品が保護すべき素材を傷付けないことを保証するか否かを決定することができる。会社Ｘ及びＺが情報を保護できるというように判定した場合には、コンテンツの提供業者は、許可されたデコーダ及び／又はプレイバック装置であるとして、Ｘ及びＺの公開キーをメディア上に記録するとともに、公開キー・フラグをセットする。この公開キーのリストは、コンテンツ・キーをメディアからプレイバック装置に転送する際に利用することができる唯一のリストであり、すなわち、承認されたデコーダ又はプレイバック装置のみがコンテンツ・キーを利用することができる。既に許可されている装置について説明してきたが、以下では、新たに承認されたり開発された装置を追加するために、このリストを更新するための方法について説明する。

【００５２】プレイバック装置は、動作中に、特定のデコーダ、例えばＸ、を使用するための暗号化されたメディア･キーを要求することがある。ドライブは、公開キー・フラグによって受理可能であることが示されたキーとしてＸを探し当てる。検索のためにキー拡張を利用する。そして、適当な公開キーを取り出して、メディア･キーを暗号化して一緒に送信する。

【００５３】許可されたデコーダのキーは、その公開キーであるので、メディア上に秘密裏に記録する必要はない。したがって、本発明の好ましい実施形態では、これらを非保護領域１０２に記録することとする。しかしながら、このような公開キーが適切に存在することによってコンテンツの有効な再生が実現されるので、これらのキーをメディアの読み出し専用（若しくは一度のみ書き込み可能な）領域に格納することによって、不心得者の不正なキーを含むように修正できないようにしておくことが好ましい。

【００５４】さらに、キーや、ひいては特定のメディアやそのコンテンツとともに使用されるデコーダの保護を実現するために、デコーダ･キー･ファイルＣＲＣ、好ましくは全てのデコーダ・キーのＣＲＣ３２、をこれらのキーの改竄を検出するために利用する。したがって、ある者がデコーダ･キー･ファイルやキー拡張を編集したり修正しようとしても、ＣＲＣは修正されたファイルに従って正されることはない。本発明の好ましい実施形態では、デコーダ･キー･ファイルＣＲＣは４バイトであるが拡張可能であり、例えば１６バイトまで拡張してＭＤ５のような他のメッセージ･ダイジェスト･アルゴリズムを使用することができる。

【００５５】安全領域に格納されているディスク･キーは、特定の適用業務に利用することができる。例えば、コンテンツ・キーのような暗号化／復号化コンテンツに利用される。公開キーの暗号化は、一般に、膨大量のデータに対しては好ましくない。何故ならば、公開キーの暗号化は、極端に遅く、且つ、プロセッサの負荷が高いからである。したがって、上述した公開キー・アルゴリズムは、ＤＥＳやＩＤＥＡ、あるいは、各端末においてキーの秘密を維持しなければならないようなその他のアルゴリズムのような、対称的な暗号化システムにおけるキーの転送に用いればよい。しかしながら、他のケースでは、ディスク･キーはメディアのコンテンツの使用を許可する際に外部ソースによって利用される識別ストリングや識別情報でもよい。以下では、このような場合にディスク･キーを使用する点について説明する。ディスク･キーの実際の形態がどのようであるかに拘らず、そのコンテンツは、暗号化されないままでは決して利用しないことが好ましい。ディスク･キー･フィールドは、５６ビットのＤＥＳキーを格納するのに充分な８バイトであることが好ましい。

【００５６】ＳＣＭＳカウントは、書き込み可能ドライブが、コピーが許可されているか否かを判別するための利用するのが好ましい。コピーが許可されている場合、ＳＣＭＳは、許容コピー生成回数に関する情報も提供する。ＳＣＭＳカウントは、メディア装置によって許可さ

れたコピーが完了する度に減分することが好ましい。例えば、以下に示すシーケンスに従って、保護ディスクをコピーすればよい。

【００５７】（１）オリジナル･ディスクを装填する。（２）ホストが、ドライブに対して、安全領域からの読み出しを命令する。許容コピー・カウント･フィールドがゼロであれば、ドライブはエラーを発生する。（３）ドライブは、安全領域から読み出した情報をキャッシュする（キャッシュされた情報はホストに返さないことが好ましい）。（４）ブランクのディスクを装填する。（５）ホストが、ドライブに対して、キャッシュされた保護領域の書き込みを命令する。（６）ドライブは、許容カウント･フィールドを減分して、ディスクのセクターに書き込みを行う。

【００５８】暗号タイプは、好ましくは、以下のテーブルに示すような、推奨使用を示したフラグである。したがって、本発明の好ましい実施形態では、異なる暗号タイプが選ばれた場合であっても、コマンドは処理動作を変えないので、全てのケースを実現するためのコマンドは、全てのケースにおいて首尾よく稼動する。例えば、本来はスタンダード･ビデオ用にデザインされたディスク＊クは、スタンダードＲＯＭ識別技術と同様のセクター･データを使用する。他の利用形態は、本来はメディア上には格納されていないものをデコーダ上で再生することを許可するためのペイ･パー･ビュー技術に利用することである。

【００５９】

【表３】暗号タイプ　　説明

0	スタンダード･ビデオ
1	ペイ･パー･ビュー
10　８０ｈ	スタンダード･データ

【００６０】地域コードは、ディスクが使用を許可された地域を示すために用いられる。各ビットは、地域に対応している。

【００６１】本発明の好ましい実施形態では、全ての暗号化情報の転送は、ＳＦＦ８０９０転送キー／レポート･キー構造に合致している。したがって、以下に示すキー・タイプ・コードが好適に利用される。キー・タイプは、ディスク上で使用される暗号化のタイプを示すものである。

【００６２】

【表４】

キー型式	説明
０ｈ	ディスクはＣＳＳに従って暗号化される
１ｈ	ディスクは本発明に係る技術によって保護される
２ｈ	予約
３ｈ	予約

【００６３】以下では、キー・タイプ１（すなわち本発明に係るキー・タイプ）について説明する。

【００６４】本発明の好ましい実施形態に従った処理動作では、ＳＦＦ８０９０レポート･キーは以下の通りで※ある。

【００６５】

【表５】

	7	6	5	4	3	2	1	0
0	オペレーション・コード							
1	LUN（古い）			保留			キー･タイプ	
2	LBA							
3								
4								
5								
6	キー・ソース							
7	保留							
8	転送長さ							
9								
10	AGID			キー・フォーマット				
11	ベンダー固有			保留		NACA	フラッグ	リンク

【００６６】但し、［表５］中で、キー･ソース及びキー･タイプ･フィールドは新規であり、コマンド空間上に存在する複数の手法に対して許容される。

【００６７】キー･ソースは、ディスク･キーのソースを以下のように示している。

【００６８】

【表６】

キー･ソース値	キー･ソース	説明
００ｈ	生成	ディスク･キーは全てゼロ
０１ｈ	生成	ディスク･キーは現在の乱数
０２ｈ	メディア	ディスク･キーは仮のディスク･キー ＡＧＩＤ許可によりゼロに初期化
０４ｈ	メディア	ディスク･キーはキー･セクタに記録
０８ｈ	メディア	ディスク･キーはＤＳＶ例外として符号化
１０ｈ	メディア	ディスク･キーはＥＣＣ例外として符号化
２０ｈ	メディア	ディスク･キーはユーザ･データ空間内
４０ｈ	メディア	ディスク･キーはキー･セクタのセクタ･ヘッダ内
８０ｈ	メディア	ディスク･キーはボーダ領域内

【００６９】通常、１又は２ビットがセットされると予想される。もし２ビットがセットされたならば、１つは現在の乱数となる。好ましい実施形態では、１よりも大きなビットがセットされたならば、ディスク･キーは要求された全てのキーの排他的論理和とする。

【００７０】キー･フォーマットは、要求されたキーの＊タイプを定義するものである。本発明の好ましい実施形態に従ったキー･フォーマットの定義を、以下の［表７］及び［表８］に示しておく。

【００７１】

【表７】

キー・フォーマット	説明
０	ＡＧＩＤの要求。ＡＧＩＤに対する乱数を再生成する （全てのキー･タイプについて共通である）
１	最も最近に送信された公開キーで暗号化されたディスク･キーを報告する。
２	メディア公開キーを報告する
３－３Ｅｈ	予約
３Ｆｈ	メディア上のキー･タイプを報告する （全てのキー･タイプについて共通である）

【００７２】送信キーの場合：　※【表８】

【００７３】　※30

キー・フォーマット	説明
１	現在の公開キーを送信する
２	ディスク･キーを送信する。ドライブは、現在のＡＧＩＤに対する仮のディスク･キーとしてこの値を格納する。

【００７４】これまでは、本発明に従ってメディアの安全な領域に格納された情報について説明してきた。以下では、このような情報をメディア上に格納する本発明の好適な実施形態について、図２を参照しながら説明する。図２には、本発明に従って記録され保護されたメディアのマスター作成又は生成する処理手順について示している。

【００７５】ステップ２０１では、素数ｐ及びｑを選択する。ｐとｑはともに５１２ビットであることが好ましい。勿論、本発明によって生成された暗号キーを破るために要する困難性に対する要求されたレベルに応じて、より大きな素数若しくはより小さな素数を本発明に適用することができる。

【００７６】ステップ２０２では、公開キーの片方半分（ｅ）が選択される。ｅは、（ｐ－１）×（ｑ－１）に対して素である。後述するように、ｅとｎの各々は、本発明の好適な実施形態における公開メディア･キーの半分ずつを構成する。値ｎは、関係式ｎ＝ｐ×ｑから導き出される。したがって、安全なコンテンツ（ｓ）、すなわち、対応する秘密キーの使用を通じてのみ復号化されるようなコンテンツは、以下の［数１］に示す関係式を用いて、クリアなコンテンツ（ｃ）から導き出される。

【００７７】

【数１】

$$s_{pub}=c^{e} \bmod n$$

【００７８】また、クリアなテキスト･コンテンツ（ｃ）は、対応する秘密キーによって暗号化された安全なコンテンツ（ｓ）から、以下の［数２］に示す関係式を用いて導き出される。

【００７９】

【数２】

$c=s_{pvt}^{e} \bmod n$

【００８０】ステップ２０３では、秘密キー（ｄ）の片方半分が、以下の［数３］に示す関係式を満足するように計算される。

【００８１】

【数３】

$$1=d\,e \bmod (p-1)(q-1)$$

【００８２】上述した公開キーと同様、ｎは、秘密キーの残り半分として利用される。したがって、上記の公開キーを用いて暗号化された安全なコンテンツ（Ｓ）は、クリアなコンテンツ（ｃ）を供給するために、以下の［数４］に示す関係式に従って復号化される。

【００８３】

【数４】

$$c=s_{pub}^{d} \bmod n$$

【００８４】また、上記の対応する公開キーを使用してのみ復号化が可能な安全なコンテンツ（ｓ）は、以下の関係式［数５］から導き出される。

【００８５】

【数５】

$$s_{pvt}=c^{d} \bmod n$$

【００８６】ステップ２０４では、ディスク･キーｋが生成される。上述したように、このキーは、ＤＥＳスタンダードに準拠した対称キーのような暗号キーであり、安全でない領域１０２に供給されるメディア１００のコンテンツを暗号化したり復号化したりするのに利用されるコンテンツ･キーである。あるいは、ディスク･キーｋは、特定のメディア若しくはコンテンツを識別する際に利用される識別情報になる。例えば、適切な復号化キー、若しくは、メディア１００のコンテンツを利用する際に有効なそれ以外の情報を供給するための、クリアリング･ハウスの外部ソースを識別するために利用される。

【００８７】ステップ２０５では、「受容可能なユーザ」のリスト、若しくは、メディアのコンテンツを利用するために許可されたデコーダ及び／又はプレイバック装置のリストがコンパイルされる。受容可能なユーザに関するリストは、これらユーザの識別情報と彼らの公開キーの両方を含んでいることが好ましい。

【００８８】ステップ２０６では、ｐ，ｑ，ｅ，及びｋの各値が、「受容可能なユーザ」のリストや、外部ソースに関するコンテンツ情報などのその他の種々雑多な情報とともに、本発明に従って動作可能なメディア装置に供給される。本発明において安全な領域１０１はアクセス制限を通してのみ受け入れられることが好ましいので、これらのパラメータが本発明の適切な処理手順に従って供給されたときのみ、本発明に従ったメディア装置はこのような情報を受け入れ且つメディア１００上に記録する、という点を理解されたい。それゆえ、本発明の好ましい実施形態では、提供業者が利用されるキーの現実のオリジネータであることを確証するためには、値ｎではなく素因数ｐ及びｑをメディア装置に供給しなければならない。

【００８９】したがって、ステップ２０７では、メディア装置は、自身に供給された値ｐ及びｑからｎを計算する。不心得者が、例えばメディア１００の安全な領域１０１に対する不正なアクセスを通じてｅやｎの値を横取りすることができたとしても、値ｐ及びｑのいずれも利用可能ではなく、且つ、不心得者は以前に生成されたキーの一部分とともに利用するのに適した値を選択することができないので、本発明に従って動作するメディア装置は、不正なコピーの実行を有効に防止することができるであろう。

【００９０】ステップ２０８では、メディア装置は、ｎ，ｅ，ｋ、及び、受容可能なユーザのリストを、メディア１００の安全な領域１０１に記録する。安全な領域に対する制限されたアクセスを提供するメディア装置に関して議論してきたが、上述した本発明は、上述したようにメディア装置とのインターフェースを持つ小さなチップのようなインテリジェンスを備えたメディア１００の一部にも適用することができる、という点を理解されたい。したがって、この情報の格納は、アクセスを制限して上記の値ｎの計算などの動作を実行するメディア装置に頼るのではなく、メディアの関連するインテリジェンスとの相互作用を介して行うことができる。

【００９１】ステップ２０９では、本発明に関する特定の実施形態がメディア１００の安全でない領域１０２に格納するコンテンツを暗号化することを含むか否かを判断する。かかるコンテンツの暗号化が望まれていない、すなわち、メディアの真正性確認にのみ暗号化が利用されているならば、処理はステップ２１４に進み、コンテンツがメディア１００に記録される。

【００９２】これに対し、このコンテンツに対する暗号化が望まれているならば、処理はステップ２１０に進み、当該実施形態が、「ペイ･パー･ビュー」サービスを提供するために利用されるクリアリング･ハウスのような外部ソースから供給される情報を利用するか否かを判断する。もし外部ソースからの情報を必要としないならば、処理はステップ２１２に進んで、コンテンツ･キーがディスク･キーにセットされる。

【００９３】メディア１００のコンテンツを利用するために外部ソースからの情報が必要である場合には、処理はステップ２１１に進み、コンテンツ･キーがランダムに選択されるか、あるいは他の適当な方法により選択される。ステップ２１１で選択されたコンテンツ･キーは、クリアリング･ハウス若しくはその他の外部エージェントに供給されて、メディア１００のコンテンツを後

に利用するために供される、という点を理解されたい。但し、このキーは、メディア１００上には格納されず、したがって、コンテンツを使用するためにクリアリング・ハウスにコンタクトする必要がある。

【００９４】外部ソースを利用するか否かに拘らず、安全でない領域１０２に格納するコンテンツは、コンテンツ・キーで暗号化してから（ステップ２１３）、メディア１００に記録する（ステップ２１４）。したがって、コンテンツ・キーでコンテンツを暗号化するために、ステップ２１１及び２１２はともに、ステップ２１３に先行する。

【００９５】上述では、本発明の好適な実施形態に従ってディスクのマスターを作成する手順について詳解してきた。以下では、図３～図５を参照しながら，本発明の好適な実施形態に従って供給されるコンテンツの利用について説明する。

【００９６】ステップ３０１では、プレイバック装置はメディア１００の暗号タイプを要求する。これに応答して、メディア装置は、メディアから暗号タイプを読み取る（ステップ３０２）。上述した本発明の好ましい実施形態では、メディアの安全な領域に記録されることになっているが、暗号タイプに関する情報はメディア上の何処に格納してもよい、という点を理解されたい。

【００９７】ステップ３０３では、メディアンのコンテンツに関して暗号が利用されているか否かを判断する。いずれの暗号も利用されていないと判断した場合には、処理はステップ３２６に進んで、本発明に従ったディスク認証を利用するか否かを判断する。

【００９８】コンテンツを保護するための暗号が利用されていると判断したときには、ステップ３０４に進んで、該暗号が「標準」であるか否かを判断する。コンテンツを保護するために利用した該暗号が標準以外であると判断された場合には、処理は、コンテンツの利用に際して外部ソースの利用に関連したステップ３１４に進むが、この点は後に詳解する。もし暗号が標準であるならば、処理はステップ３０５に進んで、「受容可能なユーザ」のリストを要求する。その後、ステップ３０６では、メディア装置は「受容可能なユーザ」のリストをメディアから読み取って、この情報をプレイバック装置に供給する。次いで，ステップ３０７において、プレイバック装置は、コンテンツ・ターゲットすなわち利用可能なデコーダのリストを生成する。

【００９９】ステップ３０８では、プレイバック装置にとって利用可能なコンテンツ・ターゲットのうちで、特定のメディアと動作することを許可されている「受容可能なユーザ」のリストに含まれているものと合致するものがあるか否かを判断する。適合するものが見つからなかった場合には、処理は、コンテンツを利用する際の外部ソースの利用と関連するステップ３１４に進んで、クリアリング・ハウスと接続したときに、適合する公開キーのリストのような情報を転送するなどによって、更新された「受容可能なユーザ」のリストを利用してもよい。新しいデコーダが製造され，若しくは特定のメディアが発行された後に許可された場合には、第三者的なプロバイダとの通信の際には該新しいデコーダの公開暗号キー方式を利用して、新しいデコーダの利用を許可することができる。

【０１００】例えば、メディア装置は、クリアリング・ハウスとの通信を確立して、リスト上の受容可能なキーすなわちメディア公開キーの１つを利用するなどによって、自分自身がコンテンツ自体を所有する人物であることをサービス・プロバイダに識別させることができる。したがって、本発明に関する技術を知る得るメディア装置は、メディア上に供給された公開キーを用いて、コンテンツ提供業者にディスク・キーを渡すことができる。このディスク・キーは、プレイバック装置が望むデコーダを識別するものであり、その引き渡しは、可能ならば、ホストに対する要求と一緒にして供給され、保護してもしなくてもよい。コンテンツ提供業者の公開キーによって暗号化された合法なディスク・キーを受信する際、コンテンツ提供業者は、合法なディスクであることを高いレベルで信用することができるし、それゆえ、特定のデコーダの許可された公開キーや、許可された公開キーのリストを、メディア上で発見されたコンテンツ提供業者の公開キーに対応する秘密キーを用いて暗号化して返信することができる。その後、メディア装置は、このキーで受信したリストを復号化することができる。

【０１０１】本発明の好ましい実施形態では、許可されたキーの取り出しは、許可された適切なキーがメディア上で発見されないときに，既に上記で概略説明したステップにおいて自動的に実行される。しかしながら、本発明の代替的な実施形態では、許可されたデコーダの更新は、メンテナンス・サイクルで実行される。例えば、夜間やプレーヤを使用しない期間などの所定の時間間隔で、オーソライズ・デコーダが更新される。

【０１０２】「受容可能なユーザ」のリストと，プレイバック装置において利用可能なコンテンツ・ターゲットのリストの間で照合が得られたならば、ステップ３０９に進んで、照合する「受容可能なユーザ」を識別するために、コンテンツ・キーの要求が送信される。ステップ３１０では、「受容可能なユーザ」のリストの中で、要求された「受容可能なユーザ」が有効化される。そして、実際に照合するものと仮定して、ディスク・キー、ここではコンテンツ・キー、がメディアから読み出され（ステップ３１１）、そして、「受容可能なユーザ」に照合する公開キーで暗号化される（ステップ３１２）。このような処理の後、ステップ３１３において、暗号化されたディスク・キーがプレイバック装置に供給されて、メディア上に記録されたコンテンツの有意義な使用が許可され、本発明に係る処理手順が完結する。ディス

ク･キーは特定のデコーダの公開キーを用いて暗号化されるので、たとえ不心得者が上述したようなステップをエミュレートしたとしても、メディア１００のコンテンツを実際に復号化できるのはこのデコーダのみである、という点を理解されたい。

【０１０３】コンテンツを保護するために利用された暗号が標準以外のものであると判定された（ステップ３０４）、若しくは、プレイバック装置において利用可能ないずれのデコーダも「受容可能なユーザ」のリストに含まれていないならば（ステップ３０８）、外部コンタクト情報がメディア上に存在するか否かを判断する（ステップ３１４）。コンタクト先である特定のクリアリング･ハウスはメディア１００のコンテンツを利用する際に必要な暗号キーを供給することができるので、この外部コンタクト情報を安全でない領域１０２に記録することができる。不正な直撃、すなわち、不心得者が外部からコンタクトするためのコンタクト情報を、本発明に従って動作するメディア１００や、メディア装置及び／又はプレイバック装置上に秘密裏に記録することによっても、メディア１００のコンテンツは打ち破られない。さらに、クリアリング･ハウスから供給される情報は、秘密メディア･キー、すなわち上述のｄ及びｎを用いて暗号化されているので、不心得者のクリアリング･ハウスは、秘密キーを得ない限り、適切な応答を行うことができない。

【０１０４】ステップ３１４において、コンタクト情報が存在しない、すなわちメディア１００のコンテンツを利用するための外部ソースに関する有効な情報が存在しないと判定されたならば、本発明に係る処理手順は完結する。他方、コンタクト情報が存在すると判定されたならば、処理はステップ３１５に進んで、外部ソースから取り出されたコンテンツ･キーがコンテンツの無制限な使用を許可するものかあるいは一回のみの使用を許可するものかを判別する。

【０１０５】もし１回の使用のみ許可されている、すなわち、使用毎に使用料の支払いが求められている場合のように、ユーザはコンテンツを利用する度に逐次的にコンテンツ･キーを要求しなければならないならば、処理はステップ３１６に進む。ステップ３１６では、乱数との排他的論理和がとられたディスク･キーの暗号化結果を要求する。次いで、ステップ３１７では、メディア装置は、乱数を生成する。乱数は、本発明に従ってランダムに選択される固有の値であり、本発明に従って１回の繰り返しを完了するのに充分な時間間隔だけ保持される。ステップ３１８では、ディスク･キーは乱数と排他的論理和がとられ、ステップ３１９では、排他的論理和がとられたディスク･キーが公開メディア・キーによって暗号化される。

【０１０６】他方、コンテンツに対する無制限な使用が許可されている場合、すなわち、１回のみの使用料の支払い若しくはメディアの許可されたコピーの検証によって、特定のプレイバック装置に関してコンテンツのキーが恒久的に解除されるような場合、若しくは、クリアリング･ハウスによって供給される情報が「許可されたユーザ」に関する更新情報である場合には、本発明に係る処理はステップ３２０に進む。ステップ３２０では、暗号化されたディスク･キーが要求される。この要求には、秘密暗号キー、若しくは、公開メディア･キーを有する誰かが返信データ･パケットを横取りしてコンテンツを復号化することを防止するための、返信パケットをさらに保護することができるその他の手段を含めて転送することができる。次いで、ステップ３１９では、公開メディア･キーを用いてディスク･キーを暗号化する。

【０１０７】プレイバック装置が１回のみ又は無制限の使用を判断することに代えて、本発明に係るメディア装置が、メディア１００に格納されている情報を参照することで、該判断を行うことができる、という点を理解されたい。かかる情報は，例えば、安全な領域１０１の予約領域に格納される。したがって、ステップ３１５においてなされた決定により、プレイバック装置は、ディスク･キーと、メディア装置キーを要求することができる。但し，メディア装置キーは、１回のみの使用が許可されている場合には乱数との排他的論理和がとられ、無制限な使用が許可された場合にはゼロとの排他的論理和がとられる。

【０１０８】ステップ３２１では、メディアを識別する情報とともに、プレイバック装置において利用可能なデコーダのリストが、暗号化されたディスク・キーに添付される。メディアを識別する情報は、上述したような予約領域内のようなメディア上の安全な領域、若しくは安全でない領域のいずれかに格納され、例えばステップ３１９において暗号化されたディスク・キーを伴うことによって、メディアから供給される、という点を理解されたい。

【０１０９】ステップ３２２において、メディアを識別する情報と、使用可能なデコーダのリストと、暗号化されたディスク・キーとが、クリアリング・ハウスに供給され、このクリアリング・ハウスからの応答を待つ。この情報パケットは、前述した一般電話回線やインターネットに接続された前述のモデムのような通信装置を利用して、プレーヤからクリアリング・ハウスに供給することができる、という点を理解されたい。もちろん、当業界において周知の他のデータ通信手段や本発明以後に開発されるデータ通信手段を、本発明に適用することができる。

【０１１０】クリアリング・ハウスは、プレーヤからデータ・パケットを受信すると、図６に記述するような処理手順に従って動作することが好ましい。図６については後述する。メディア１００のコンテンツとともに使用するのに適したコンテンツ・キーが、上述した秘密メデ

ィア・キーによって暗号化された形態で、プレーヤに返されることが好ましい。

【０１１１】ステップ３２３では、クリアリング・ハウスからの応答が、メディア装置に供給され、公開メディア・キーを用いて復号化される（ステップ３２４）。上述したように、本発明の実施形態では、１回だけ使用する場合には、乱数が利用される。この乱数は、クリアリング・ハウスにおいて、プレーヤに供給するコンテンツ・キーの排他的論理和をとるために利用される。本発明によれば、コンテンツ・キーを引き出す際にメディア装置が乱数を要求するが、本発明によれば、乱数は一度使用すると廃棄されてしまう。このため、不心得者は、コンテンツの繰り返し利用のためにプレーヤに後に再提出するために、クリアリング・ハウスから返されるパケットを単純に捕捉することができない。さらに、メディア公開キーを所持する者であっても、乱数を知らなければ、データ・パケットを復号化したり、さらにコンテンツ・キーを取り出すことができない。したがって、単一の使用のみが許可された場合に実行されるステップ３２４では、復号化された情報と乱数との排他的論理和をとることによって、コンテンツ・キー及び／又は供給されるその他の情報を露わにすることができる。

【０１１２】ステップ３２５では、繰り返し使用のためのコンテンツ・キーがメディア装置に格納されるので、後続の使用のために、新規な若しくは更新された「受容可能なユーザ」のリストを格納することができる。クリアリング・ハウスから供給されたコンテンツ・キーは、多数回使用のためにメディアのキーを解除するのに有効であり、すなわち、本発明に係る１回の使用のみのために保持される乱数でキーの排他的論理和をとらなくてもよい。プレイバック装置、若しくは他のホストは、適当な時間にメディア装置に対して後続の供給を行うためのデータ・パケットを記憶してもよい。

【０１１３】「受容可能なユーザ」のリストの更新に関して既に述べたが、本発明は、本発明ではもはや受容できない公開キー・フラグ及び／又はキー拡張によって許可されたものと識別されたデコーダのうち特定の１つを指示するように動作することができる、という点を理解されたい。例えば、ある特定の秘密キーが破られた場合、クリアリング・ハウスから受け取る更新情報が公開キーの１つがもはや使用不可であることを指示するようにしてもよい。したがって、ステップ３０６において、このような「解約」リストに関するチェックが実行され、かかる秘密キーの使用を不許可にする。

【０１１４】上述のようにしてステップ３０５から３１３に至るまでの処理が進行する。しかしながら、「ペイ・パー・ビュー」におけるクリアリング・ハウスからのデータ・パケットの中にコンテンツ・キーが含まれている場合には、ステップ３１１では、メディア上に格納されたディスク・キーではなくて、このコンテンツ・キーを利用する、という点を理解されたい。同様に、「受容可能なユーザ」のリストを更新するために外部情報を利用する場合には、ステップ３０６における情報はクリアリング・ハウスから供給された更新情報を含む。

【０１１５】クリアリング・ハウスから得られるコンテンツ・キー及び／又は更新された「受容可能なユーザ」リストは、必要に応じてメディア１００内に格納することができる、という点を理解されたい。しかしながら、この情報を不正に記録すると、本発明に従って提供される保護を解除するために使用されかねないので、この情報をメディアに記録する場合には、安全な領域に記録することが好ましい。

【０１１６】ステップ３０３において、メディア１００のコンテンツを保護するために使用された暗号がないと判定されたならば、次いで、ステップ３２６において、本発明に従ったディスク認証が利用されたか否かを判定する。ディスク認証が利用されていない場合には、本発明に係る処理動作は完結し、この結果、プレイバック装置はメディア１００のコンテンツを利用する運びとなる。

【０１１７】他方、ディスク認証が利用されている場合には、ステップ３２７に進んで、プレイバック装置は乱数を発生する。そして、プレイバック装置は、この乱数を秘密メディア・キーで暗号化する（ステップ３２８）。暗号化された乱数は、ステップ３２９において、メディア装置に転送される。そして、メディア装置は、メディア１００の安全な領域に格納されている公開メディア・キーを用いて乱数を復号化する。

【０１１８】プレイバック装置は、乱数を、メディア１００の安全な領域に格納されているディスク・キーで排他的論理和をとることを要求する（ステップ３３１）。これに応答して、ステップ３３２において、メディア装置は乱数をディスク・キーで排他的論理和をとる。次いで、メディア装置は、乱数とディスク・キーとの排他的論理和の結果をメディア公開キーで暗号化して、このデータ・パケットをプレイバック装置に供給する（ステップ３３３）。プレイバック装置は、秘密メディア・キーを用いて、排他的論理和された乱数とディスク・キーを復号化して（ステップ３３４）、この復号化された情報を乱数で排他的論理和をとる（ステップ３３５）。

【０１１９】ステップ３３６では、上述の各ステップによって得られたディスク・キーが期待された若しくは既知のディスク・キーと一致するか否かを判定する。もし一致するならば、メディアは真正、すなわち、非保護領域１０２内に供給された情報の単純なコピーは行われていなかったことになる。他方、ディスク・キーが一致しなければ、メディアは真正でないことになる。

【０１２０】上記の本発明の好ましい実施形態では、標準的な暗号方式と、外部の認証、及び、メディア認証を単一の実施形態の中で利用すると説明したが、これらの

技術のうちいずれかを組み合わせて利用してもよいという点を理解されたい。例えば、ペイ・パー・ビュー専用の装置の場合であれば、システムは上記のうち外部認証に関連するステップのみを該システム上で実行すれば充分である。同様に、メディア認証を行わないと予想される場合であれば、装置は、標準的な暗号方式と外部認証に関連するステップのみを実行するように装置を構成することができる。

【０１２１】図６には、クリアリング・ハウスがプレーヤからの要求に応答して実行する、本実施例に係る処理手順について図解している。ステップ４０１では、クリアリング・ハウスは、プレーヤがステップ３２２において送信したデータ・パケットを受信する。データ・パケットは、メディア１００に格納されている公開メディア・キーに対応する秘密メディア・キーを用いて復号化される（ステップ４０２）。ステップ４０３では、受信したデータ・パケットに含まれる情報を用いて、特定のメディアが識別される。クリアリング・ハウスは、メディアを明示的には指定しない利用可能な情報を通して特定のメディアを識別することができる、という点を理解されたい。例えば、特定の公開キーによってメディアを充分に同定することができる。同様に、例えば要求元プレーヤのＵＲＬ（Uniform ResourceLocator）あるいはＡＮＩ（Automatic Numbeer Identification）のような、通信を介して収集される情報は、本発明において利用することができる。

【０１２２】ステップ４０４では、クリアリング・ハウスは、復号化されたディスク・キーと、メディア装置によってディスク・キーと排他的論理和された乱数とを排他的論理和することによって、メディア装置によって生成された乱数を回復する。この乱数は、コンテンツ・キーを排他的論理和するために利用される。すなわち、プレーヤに供給されて、メディア１００の暗号化されたコンテンツを有意義に使用するために、プレイバック装置において利用される。ステップ４０６では、プレーヤに供給される情報には、「受容可能なユーザ」のリスト、若しくはその更新されたリストを添付してもよい。次いで、プレーヤに供給すべき情報が、秘密メディア・キーを用いて暗号化されて（ステップ４０７）、プレーヤに送信される（ステップ４０８）。

【０１２３】メディアのファイル・システム情報は暗号化しない方が好ましい。但し、ファイル中のデータは、コンテンツ・キーを用いて暗号化してもよい。したがって、制御ファイルは、どのファイルが暗号化されていてどれが暗号化されいないか表示することが好ましい。かかる表示によって、同一のメディア上に、保護された情報と自由に配布できる情報とを共存させることができる。例えば、映画のような特定のコンテンツのみを保護する一方で、プロモーション用の広告編のようなそれ以外のコンテンツを保護せずに配布可能な状態におくことができる。

【０１２４】本発明の実施形態では、暗号化の処理手順は、メディアの各セクタ毎に再スタートすることが好ましい。かかる処理手順によって、メディアにおけるセクタ毎のアドレス指定可能を維持することができ、メディア上で今日供されているコンテンツに対するランダム・アクセスが可能になる。

【０１２５】上述したように、本発明に従って動作するメディア装置によれば、安全な領域内に許可された情報書き込みを行うことによって、保護コンテンツの生成を行うことができる。但し、不心得者がこのような安全な領域にアクセスすることによって合法的に作成されたマスター・メディアを改竄することを防止するために、メディア・キー（ｎ）の因子である２つの素数を供給することによって、かかる安全領域への書き込みを行うようにする。ディスク・キーは、送信された公開キーに対応する秘密キーを用いて暗号化した状態で供給される。メディア装置は、２つの素数を乗算して、その積をメディア・キー（ｎ）フィードに記録する。メディア装置は、入力数値が素数であることを検証する必要はない。ユーザは、安全でないキーを生成するが、安全なキーを再生成することはできない。メディア装置がメディア上に記録を行うためのディスク・キーが、素数ｐ及びｑから計算された公開メディア・キーを用いて復号化することによって得られる。

【０１２６】したがって、著作者が当該素数を持つことによって、保護ディスクの著作が可能となる。対応する素因数を知らずしてこのキーを書き込むことはできないので、不正なコピー操作は決して成功することはない。たとえ、ユーザがこれらのキーを入手できたとしても、これらを記録することはできない。

【０１２７】商業上の書き込みは、上記に従って行うことができる。但し、さらに保護を強化するためには、素数そのものを１０２４ビットにするか、あるいは、一方の素数が５１２ビットよりも大きな２つの素数の積を１０２４ビットにしてもよい。これによって、一般消費者レベルの製品に関しても、たとえキーを因数分解することができたとしても、キーのコピーを防止することができる。

【０１２８】専用のプレーヤが安全な領域からディスク・キーを読み取ることによって、専用のプレーヤ上で本発明を実装することができる、という点を理解されたい。ペイ・パー・ビュー方式がサポートされているならば、専用のプレーヤは、上述したように公開キー・プロトコルを実装してもよい。

【０１２９】さらに、コンピュータ・システム上でも本発明を実装することができる、という点も理解されたい。但し、コンピュータ・システム内で通常見出されるＲＯＭドライブは、ホスト・インターフェース経由で配布されたデータの復号化を行わない。復号化に基づくＭ

ＰＥＧデコーダが使用され、復号化は、ドライブから供給されたキーを用いてＭＰＥＧデコーダによって行われることが好ましい。コンテンツの保護を維持するためには、ＭＰＥＧデコーダは記録を許可するいかなるインターフェースに対してもコンテンツを配布すべきでない。

【０１３０】上述した例では、ＤＶＤフォーマットのバルク格納装置について議論してきたが、いかなるタイプのバルク格納装置に対しても上述した技術を適用することができる、という点を理解されたい。例えば、本発明に係る技術は、ＣＤ－ＲＯＭフォーマットのバルク格納装置に対しても、安全な領域は何処に隠されているかとか、読み取り不可である旨をどのようにマークするかとか、ディスク・キーをどうやって隠すかといった単純な相違だけで、適用することができる。

【０１３１】付言するならば、本発明の好適な実施形態によれば、上述したように、ホスト又はドライブに関する固有の識別子を必要としない、という点も理解されたい。このため、アップグレードや故障などに伴ない、ハードウェアを交換することができる。

【０１３２】これまで本発明及びその利点について記述してきたが、［特許請求の範囲］の欄に記載された各請求項によって定義された本発明の要旨や範囲を逸脱することなく、様々の変更や代替、修正等を行い得るという点を理解されたい。

【０１３３】この発明は、例として次の実施態様を含む。

（１）格納メディアに格納されたコンテンツの無権限の使用を防止するためのコンテンツ保護方法であって、メディアの使用を許可された少なくとも１つの装置に関する情報を含んだ第１の情報を、該メディア上のアクセスが制限された部分に格納するステップと、許可された前記少なくとも１つの装置の暗号キーを含んだ第２の情報を該メディア上に格納するステップと、ユーザ・コンテンツを該メディア上のアクセスが自由な部分に格納するステップと、特定のメディア使用装置が前記ユーザ・コンテンツを供給するのに受容可能なメディア使用装置であるか否かを、前記第１の情報の少なくとも部分的に参照することによって判断するステップと、前記特定のメディア使用装置が前記判断ステップにおいて受容可能と判断されたか否かを含んだ情報を、前記第２の情報に含まれる前記暗号キーで暗号化して、前記特定のメディア使用装置に転送することによって、前記特定のメディア装置が前記ユーザ・コンテンツの少なくとも一部を使用することを可能にするステップと、を備えるコンテンツ保護方法。

【０１３４】（２）さらに、前記コンテンツ情報が暗号化されているか否かを判断するステップと、前記コンテンツ情報の暗号が外部接続装置における復号化に利用されるか否かを判断するステップと、前記コンテンツ情報の前記暗号が外部接続装置において利用されると判断された場合において、前記特定のメディア使用装置が前記ユーザ・コンテンツを利用することを可能にする際に有効な情報を持つ外部接続装置との接続を確立するステップと、前記特定のメディア使用装置が前記ユーザ・コンテンツを利用することを可能にするために有効な前記の情報を取り出すステップとを具備し、前記の可能にするステップにおいて前記特定のメディア使用装置に転送された前記の情報は前記の取り出された情報の少なくとも一部を含む、上記１に記載のコンテンツ保護方法。

【０１３５】（３）前記の特定のメディア使用装置が受容可能なメディア使用装置であるか否かを判断するステップは、前記特定のメディア使用装置が受容可能なメディア使用装置であることを前記第１の情報が表示しているか否かを再調査するステップと、該メディアに関する外部接続情報が利用可能か否かを判断するステップと、前記外部接続情報が利用可能であると判断された場合に、前記外部接続装置との接続を確立するステップと、特定のメディア使用装置が受容可能なメディア使用装置であるか否かを判断することに関連する前記第１の情報の補足的な情報を取り出すステップと、を含む上記（１）に記載のコンテンツ保護方法。

【０１３６】（４）前記第１の情報を格納するステップは、前記第１の情報に関するパラメータを所定のフォーマットで供給するステップと、前記パラメータから前記第１の情報の少なくとも一部を引き出すステップとを含み、前記パラメータすなわち前記第１の情報の一部は前記第１の情報の前記部分の廃棄された派生語である上記（１）に記載のコンテンツ保護方法。

（５）該メディアの前記アクセスが制限された部分は、前記メディアの前記アクセス自由な部分に所定の方式で散在している上記（１）に記載のコンテンツ保護方法。

（６）該メディアの前記アクセスが制限された部分は、該メディアの活動的な部分である上記（１）に記載のコンテンツ保護方法。

【０１３７】（７）格納装置上に格納されたコンテンツの無権限の使用を防止するためのコンテンツ保護方法であって、公開暗号キーを含んだ第１の情報を、該格納装置上のアクセスが制限された部分に格納するステップと、ユーザ・コンテンツを該格納装置上のアクセスが自由な部分に格納するステップと、前記第１の情報の少なくとも一部を利用して、当該方法に従って動作することができる特定の装置を当該方法に係る使用が受容可能であるとして有効化するステップと、前記特定の装置が前記の有効化するステップにおいて受容可能であると有効化されている場合に、前記ユーザ・コンテンツの利用を可能にするステップと、を含むコンテンツ保護方法。

【０１３８】（８）前記の有効化するステップは、前記第１の情報の公開暗号キーに対応する秘密暗号キーを用いて情報を暗号化するステップと、前記第１の情報の前記公開暗号キーに対応する前記秘密暗号キーを用いて暗

号化された情報を、前記第１の情報の前記公開暗号キーを用いて復号化するステップと、を含む（７）に記載のコンテンツ保護方法。

（９）さらに、前記の許可されたメディア使用装置の少なくとも１つが持つ暗号キーを含んだ第２の情報をメディア上に格納するステップを含む上記（７）に記載のコンテンツ保護方法。

【０１３９】（１０）バルク格納装置上に保護されたコンテンツを供給するためのコンテンツ保護システムであって、少なくとも一部はアクセス制限された記憶容量として割り当てられ、且つ、他の少なくとも一部はアクセス自由な記憶容量として割り当てられた情報記憶容量を供給する格納装置と、前記アクセス制限された記憶容量に対するアクセスが許可されている状態を定義するインストラクション・セットの制御下で動作するプロセッサとを具備し、前記インストラクション・セットに従った前記プロセッサの制御下で、少なくとも格納装置の公開キーと受容可能な複数のプレイバック装置に関する情報が前記アクセス制限された記憶容量に格納されている、コンテンツ保護システム。

【０１４０】

【発明の効果】以上詳記したように、本発明によれば、記録メディア上に格納されたコンテンツを好適に保護することができる、優れたコンテンツ保護方法及び保護システムを提供することができる。

【０１４１】また、本発明によれば、記録メディア自身に格納された公開キーを用いて記録メディア上のコンテンツの使用を好適に制御することができる、優れたコンテンツ保護方法及び保護システムを提供することができる。

【図面の簡単な説明】

【図１】本発明の実施に供されるメディア･システムを図解したものである。

＊【図２】本発明の好適な実施形態に従って保護されるコンテンツを含んだディスクに対する記録動作の処理手順を示したフロー･ダイアグラムである。

【図３】本発明の好適な実施形態に従って保護されたコンテンツを利用するための動作手順を示したフロー･ダイアグラムである。

【図４】本発明の好適な実施形態に従って保護されたコンテンツを利用するための動作手順を示したフロー･ダイアグラムである。

【図５】本発明の好適な実施形態に従って保護されたコンテンツを利用するための動作手順を示したフロー･ダイアグラムである。

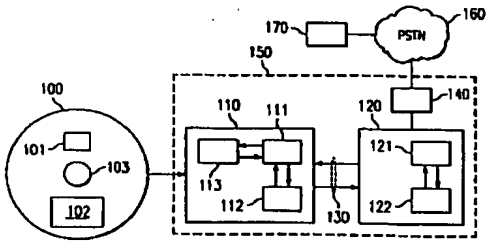
【図６】本発明の好適な実施形態に従った外部のオーソリゼイション･センタの処理動作を示したフロー･ダイアグラムである。

【符号の説明】

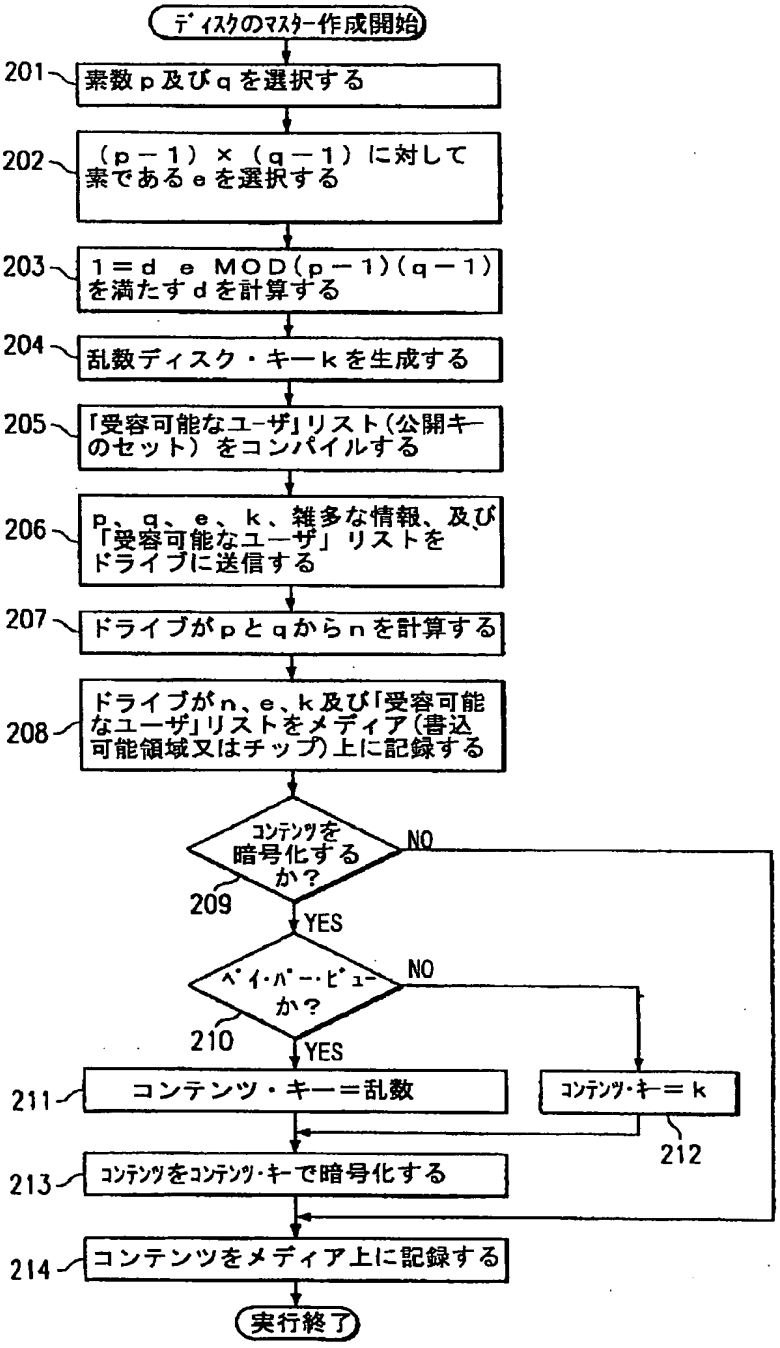
１００…メディア
１０１…保護記憶領域
１０２…非保護記憶領域
１０３…ハブ
１１０…メディア装置
１１１…プロセッサ（ＣＰＵ）
１１２…メモリ
１１３…インターフェース
１２０…プレイバック装置
１２１…プロセッサ
１２２…メモリ
１３０…バス
１４０…通信装置
１５０…プレーヤ
１６０…ＰＳＴＮ
１７０…クリアリング・ハウス

＊

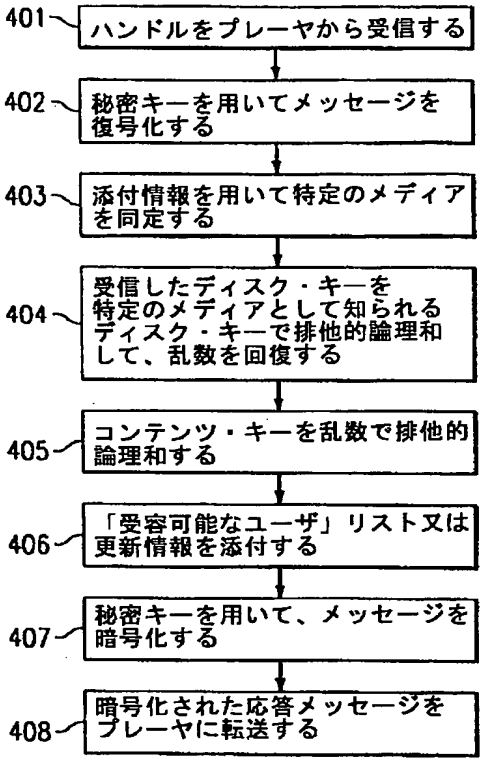
【図１】



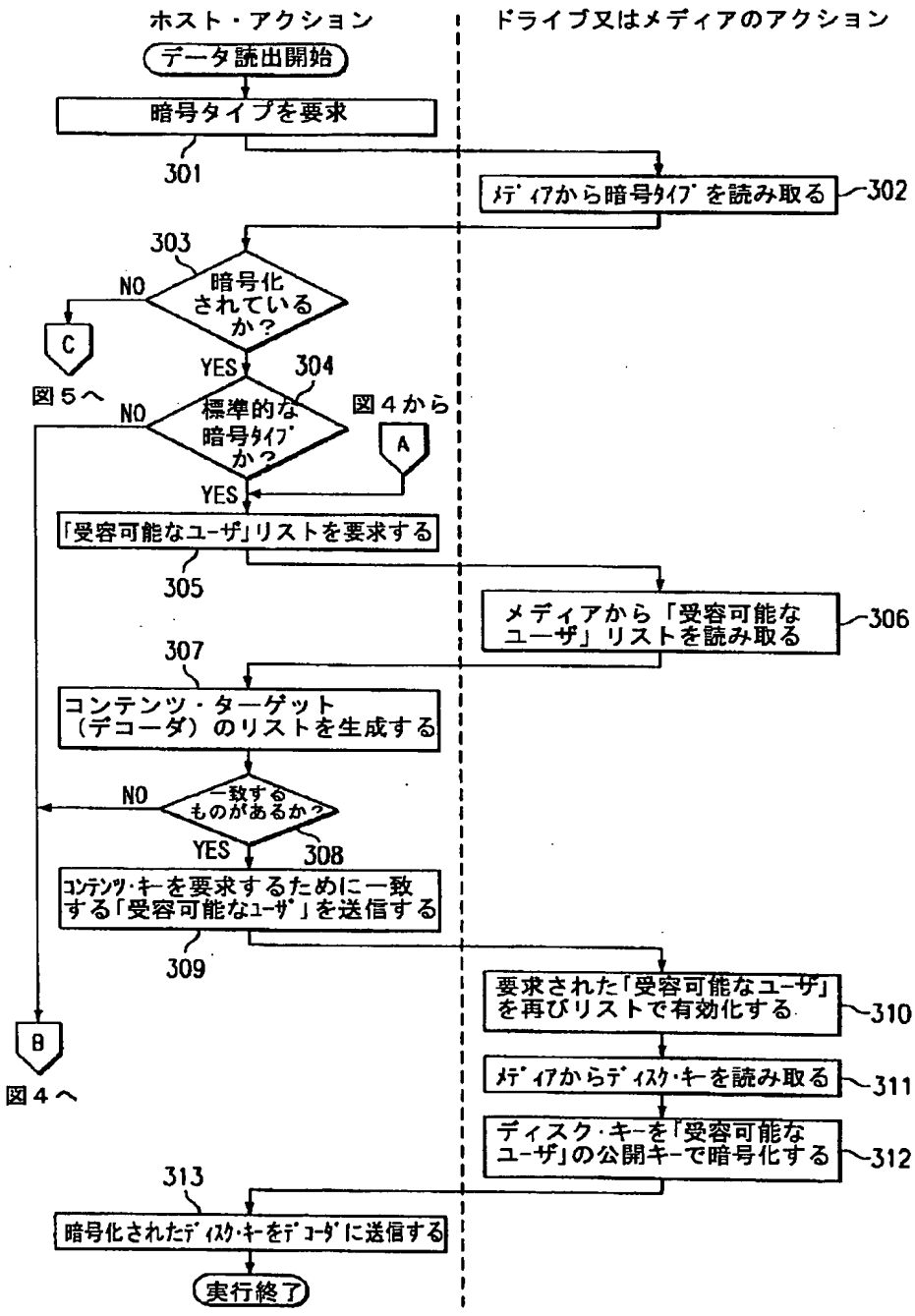
【図２】


ディスクのマスター作成開始
201
素数ｐ及びｑを選択する
202
（ｐ－１）×（ｑ－１）に対して素であるｅを選択する
203
１＝ｄ　ｅ　ＭＯＤ（ｐ－１）（ｑ－１）を満たすｄを計算する
204
乱数ディスク・キーｋを生成する
205
「受容可能なユーザ」リスト（公開キーのセット）をコンパイルする
206
ｐ、ｑ、ｅ、ｋ、雑多な情報、及び「受容可能なユーザ」リストをドライブに送信する
207
ドライブがｐとｑからｎを計算する
208
ドライブがｎ、ｅ、ｋ及び「受容可能なユーザ」リストをメディア（書込可能領域又はチップ）上に記録する
コンテンツを暗号化するか？
209
NO
YES
ペイ・パー・ビュー か？
210
NO
YES
211
コンテンツ・キー＝乱数
コンテンツ・キー＝ｋ
212
213
コンテンツをコンテンツ・キーで暗号化する
214
コンテンツをメディア上に記録する
実行終了

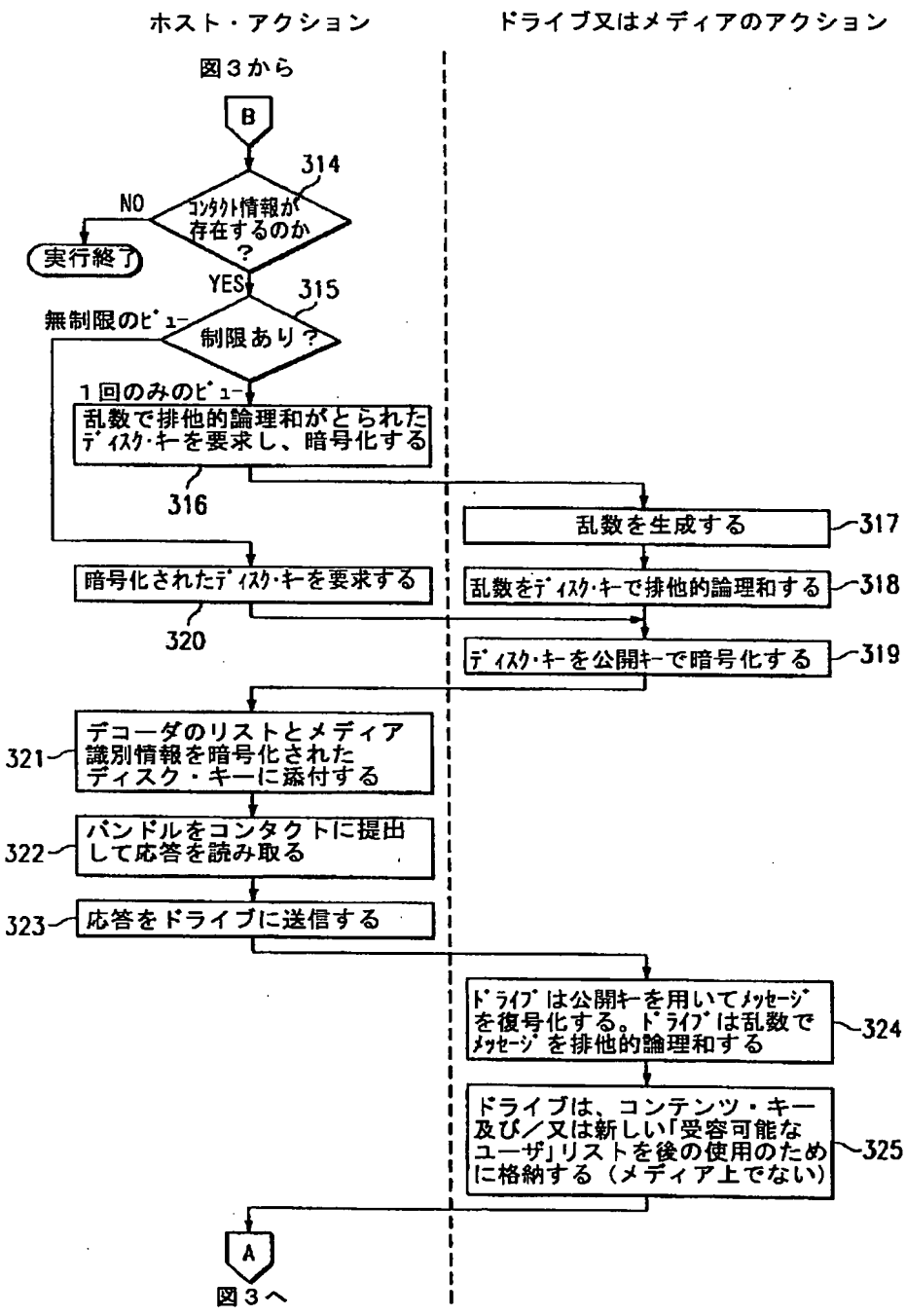
【図６】


401
ハンドルをプレーヤから受信する
402
秘密キーを用いてメッセージを復号化する
403
添付情報を用いて特定のメディアを同定する
404
受信したディスク・キーを特定のメディアとして知られるディスク・キーで排他的論理和して、乱数を回復する
405
コンテンツ・キーを乱数で排他的論理和する
406
「受容可能なユーザ」リスト又は更新情報を添付する
407
秘密キーを用いて、メッセージを暗号化する
408
暗号化された応答メッセージをプレーヤに転送する

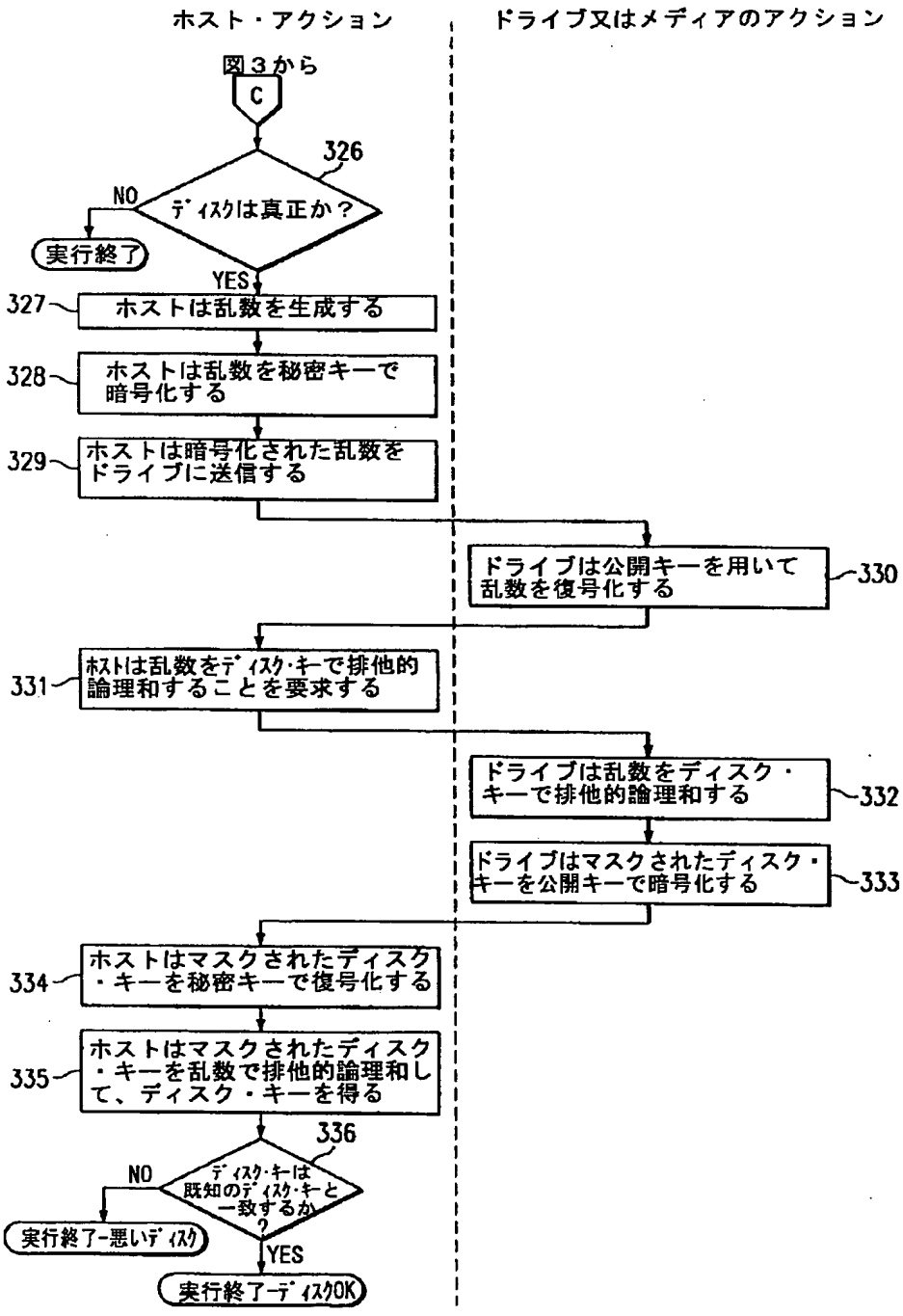
【図３】


ホスト・アクション
ドライブ又はメディアのアクション
データ読出開始
暗号タイプを要求
301
ﾒﾃﾞｨｱから暗号ﾀｲﾌﾟを読み取る
302
303
暗号化されているか？
NO
YES
C
図５へ
304
標準的な暗号ﾀｲﾌﾟか？
NO
YES
図４から
A
「受容可能なユーザ」リストを要求する
305
メディアから「受容可能なユーザ」リストを読み取る
306
307
コンテンツ・ターゲット（デコーダ）のリストを生成する
一致するものがあるか？
NO
YES
308
ｺﾝﾃﾝﾂ･ｷｰを要求するために一致する「受容可能なﾕｰｻﾞ」を送信する
309
B
図４へ
要求された「受容可能なユーザ」を再びリストで有効化する
310
ﾒﾃﾞｨｱからﾃﾞｨｽｸ･ｷｰを読み取る
311
ディスク･キーを「受容可能なユーザ」の公開キーで暗号化する
312
313
暗号化されたﾃﾞｨｽｸ･ｷｰをﾃﾞｺｰﾀﾞに送信する
実行終了

【図４】


ホスト・アクション
ドライブ又はメディアのアクション
図３から
B
314
NO
ｺﾝﾀｸﾄ情報が存在するのか？
実行終了
YES
315
無制限のﾋﾞｭｰ
制限あり？
１回のみのﾋﾞｭｰ
乱数で排他的論理和がとられたﾃﾞｨｽｸ･ｷｰを要求し、暗号化する
316
乱数を生成する
317
暗号化されたﾃﾞｨｽｸ･ｷｰを要求する
乱数をﾃﾞｨｽｸ･ｷｰで排他的論理和する
318
320
ﾃﾞｨｽｸ･ｷｰを公開ｷｰで暗号化する
319
321
デコーダのリストとメディア識別情報を暗号化されたディスク・キーに添付する
322
バンドルをコンタクトに提出して応答を読み取る
323
応答をドライブに送信する
ﾄﾞﾗｲﾌﾞは公開ｷｰを用いてﾒｯｾｰｼﾞを復号化する。ﾄﾞﾗｲﾌﾞは乱数でﾒｯｾｰｼﾞを排他的論理和する
324
ドライブは、コンテンツ・キー及び／又は新しい「受容可能なユーザ」リストを後の使用のために格納する（メディア上でない）
325
A
図３へ

【図５】


ホスト・アクション
ドライブ又はメディアのアクション
図３から
C
326
NO
ディスクは真正か？
実行終了
YES
327
ホストは乱数を生成する
328
ホストは乱数を秘密キーで暗号化する
329
ホストは暗号化された乱数をドライブに送信する
ドライブは公開キーを用いて乱数を復号化する
330
331
ホストは乱数をディスク・キーで排他的論理和することを要求する
ドライブは乱数をディスク・キーで排他的論理和する
332
ドライブはマスクされたディスク・キーを公開キーで暗号化する
333
334
ホストはマスクされたディスク・キーを秘密キーで復号化する
335
ホストはマスクされたディスク・キーを乱数で排他的論理和して、ディスク・キーを得る
336
NO
ディスク・キーは既知のディスク・キーと一致するか？
実行終了-悪いディスク
YES
実行終了-ディスクOK

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成17年7月14日(2005.7.14)

【公開番号】特開2000-138664(P2000-138664A)
【公開日】平成12年5月16日(2000.5.16)
【出願番号】特願平11-214972
【国際特許分類第７版】
　Ｈ０４Ｌ　 9/08
　Ｇ０６Ｆ　12/14
　Ｇ０６Ｆ　17/60
　Ｇ０９Ｃ　 1/00
【ＦＩ】
　Ｈ０４Ｌ　 9/00　　６０１Ｃ
　Ｇ０６Ｆ　12/14　　３２０Ｅ
　Ｇ０９Ｃ　 1/00　　６２０Ｚ
　Ｇ０９Ｃ　 1/00　　６４０Ｂ
　Ｇ０６Ｆ　15/21　　Ｚ

【手続補正書】
【提出日】平成16年11月24日(2004.11.24)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　媒体に格納されたコンテンツへの無権限のアクセスを防止する方法であって、
　特定の再生装置のタイプを示す識別子を含む特定の再生装置から、媒体に格納されたコンテンツにアクセスする要求を受け取るステップと、
　前記識別子を権限のある再生装置のタイプのリストと突き合わせるステップと、を含み、前記リストは前記媒体に格納され、前記識別子が前記権限のある再生装置のタイプのリストの中の一つのエントリと合致するとき、
　（ｉ）　前記媒体から前記一つのエントリに関連するパブリックキーを検索するステップと、
　（ii）　前記媒体から前記コンテンツの暗号化に使用されるコンテンツキーを検索するステップと、
　（iii）　前記コンテンツキーを前記パブリックキーで暗号化するステップと、
　（iv）　前記暗号化されたコンテンツキーを前記特定の再生装置に通信するステップと、
を含む方法。
【請求項２】
　前記媒体を読み出すドライブユニットを制御し、前記特定の再生装置が前記コンテンツキーを含む前記媒体の部分に直接アクセスすることを防止するステップをさらに含む請求項１記載の方法。
【請求項３】
　コンテンツの無権限の使用を防止するシステムであって、
　前記媒体に格納されたアクセス情報と特定の再生装置から受け取った検証情報とを使用して、媒体に格納されたコンテンツへのアクセスを制御する命令の組の下で動作するプロ

セッサと、
前記媒体に格納された媒体暗号化キーで暗号化された前記コンテンツと、
複数の権限のある再生装置のタイプの識別子のリストを含む前記アクセス情報と、を含み、
前記アクセス情報は、前記複数の権限のある再生装置のタイプの中の権限のある各再生装置のタイプについての各装置の暗号化キーをさらに含み、
前記命令の組は、前記媒体の前記コンテンツの読み取り要求において、前記特定の再生装置から前記検証情報を受け取るコードを含み、
前記命令の組は、受け取った前記検証情報が前記識別子のリストの中の識別子の一つと合致するかを判定するコードを含み、
前記命令の組は、前記検証情報が前記識別子の一つと合致したとき、前記特定の再生装置のタイプに関連する各装置の暗号化キーによって暗号化された前記媒体暗号化キーを前記特定の再生装置に通信するコードを含む、
前記システム。
【請求項４】
前記プロセッサは、前記媒体から情報を回復するドライブユニットを制御する請求項３に記載のシステム。
【請求項５】
前記プロセッサは、前記再生装置を前記媒体暗号化キーを格納する前記媒体の部分に直接アクセスすることを防止することによって前記ドライブユニットを制御する請求項４に記載のシステム。
【請求項６】
コンテンツの無権限のアクセスを防止する方法であって、
コンテンツをコンテンツキーで暗号化された媒体上に格納するステップと、前記コンテンツキーは前記媒体に格納され、前記媒体は多数に分散しており、
前記媒体上の権限のある媒体再生タイプを示す情報を格納するステップと、
前記媒体上の権限のある媒体再生タイプのうちの権限のある各媒体再生タイプについて各パブリックキーを格納するステップと、
特定のメディア・プレーヤから、前記媒体のコンテンツへのアクセスの要求を受け取るステップと、前記要求は、前記特定のメディア・プレーヤの特定のタイプの識別子を含み、
前記識別子と権限のあるメディア・プレーヤのタイプを示す前記情報とを突き合わせて、前記特定のメディア・プレーヤを検証するステップと、
前記検証するステップにおいて前記特定のメディア・プレーヤに権限があるとき、前記特定のメディア・プレーヤに関連する各パブリックキーによって暗号化されたコンテンツキーを前記特定の媒体プレーヤに送るステップと、
を含む方法。
【請求項７】
ドライブユニットを制御して前記媒体に格納されたデータにアクセスするステップをさらに含む請求項６に記載の方法。
【請求項８】
前記ドライブユニットの制御は、前記特定のメディア・プレーヤが前記コンテンツキーを格納する媒体の部分に直接アクセスすることを防止する、請求項７に記載の方法。